

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

06.07.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 7月 6日

出願番号

Application Number:

平成11年特許願第192413号

出願人

Applicant(s):

ソニー株式会社

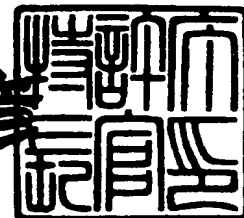
**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 6月 9日



特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3043005

【書類名】 特許願

【整理番号】 9900560711

【提出日】 平成11年 7月 6日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 野中 聡

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 江崎 正

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100094053

 【弁理士】

 【氏名又は名称】 佐藤 隆久

【手数料の表示】

 【予納台帳番号】 014890

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ提供システムおよびその方法と管理装置

【特許請求の範囲】

【請求項 1】

データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明するデータ提供システム。

【請求項 2】

前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 1 に記載のデータ提供システム。

【請求項 3】

前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、

前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 2 に記載のデータ提供システム。

【請求項 4】

前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理

装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う

請求項 1 に記載のデータ提供システム。

【請求項 5】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 1 に記載のデータ提供システム。

【請求項 6】

データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

データ提供システム。

【請求項 7】

前記データ提供装置は、前記コンテンツデータおよび前記コンテンツ鍵データを格納したモジュールを、前記データ処理装置に配給する

請求項 6 に記載のデータ提供システム。

【請求項 8】

コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

管理装置。

【請求項 9】

前記データ提供装置から、前記権利書データと、当該データ提供装置の識別子と、少なくとも前記権利書データに対して当該データ提供装置の秘密鍵データを用いて作成した署名データとを格納したモジュールを用いた前記要求を受ける場合に、

前記データ提供装置の秘密鍵データに対応する公開鍵データを管理する

請求項 8 に記載の管理装置。

【請求項 10】

前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ提供装置に送信する

請求項 9 に記載の管理装置。

【請求項 11】

コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該コンテ

ンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータを前記コンテンツ鍵データを用いて復号した後に当該コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

管理装置。

【請求項 12】

データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明するデータ提供システム。

【請求項 13】

前記データ提供装置は、前記コンテンツデータの識別子と、前記権利書データと、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 12 に記載のデータ提供システム。

【請求項 14】

前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給する

請求項 1 3 に記載のデータ提供システム。

【請求項 1 5】

前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ配給装置に提供し、

前記データ処理装置は、前記データ配給装置から配給を受けた前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う

請求項 1 2 に記載のデータ提供システム。

【請求項 1 6】

前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する

請求項 1 2 に記載のデータ提供システム。

【請求項 1 7】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益

分配処理を行う

請求項 1 2 に記載のデータ提供システム。

【請求項 1 8】

前記データ処理装置は、前記データ配給装置と通信を行う第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2 のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第 2 のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 1 2 に記載のデータ提供システム。

【請求項 1 9】

データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データおよび前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明

する

データ提供システム。

【請求項 20】

前記データ提供装置は、前記コンテンツ鍵データを暗号化し、当該暗号化したコンテンツ鍵データと前記暗号化したコンテンツデータとを格納したモジュールを前記データ配給装置に提供する

請求項 19 に記載のデータ提供システム。

【請求項 21】

コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

管理装置。

【請求項 22】

前記コンテンツデータをコンテンツ鍵データを用いて暗号化して前記データ提供装置から前記データ配給装置に提供する場合に、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

請求項 21 に記載の管理装置。

【請求項 23】

前記価格データを前記コンテンツデータおよび前記権利書データと共に、前記データ配給装置から前記データ処理装置に配給する場合に、

前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する
請求項 21 に記載の管理装置。

【請求項 24】

データ提供装置、データ処理装置および管理装置を用いたデータ提供方法にお

いて、

コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する

データ提供方法。

【請求項 2 5】

データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給し、

前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、

前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する

データ提供方法。

【請求項 2 6】

データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記権利書データの正当性を証明する

データ提供方法。

【請求項 2 7】

データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する

データ提供方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンテンツデータを提供するデータ提供システムおよびその方法と、これらに用いられる管理装置とに関する。

【0 0 0 2】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来の EMD (Electronic Music Distribution: 電子音楽配信) システムがある。

【0 0 0 3】

図 6 7 は、従来の EMD システム 7 0 0 の構成図である。

図 67 に示す EMD システム 700 では、コンテンツプロバイダ 701 a, 701 b が、サービスプロバイダ 710 に対し、コンテンツデータ 704 a, 704 b, 704 c と、著作権情報 705 a, 705 b, 705 c とを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報 705 a, 705 b, 705 c には、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ 710 の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】

サービスプロバイダ 710 は、受信したコンテンツデータ 704 a, 704 b, 704 c と、著作権情報 705 a, 705 b, 705 c とをセッション鍵データを用いて復号する。

そして、サービスプロバイダ 710 は、復号したあるいはオフラインで受け取ったコンテンツデータ 704 a, 704 b, 704 c に、著作権情報 705 a, 705 b, 705 c を埋め込んで、コンテンツデータ 707 a, 707 b, 707 c を生成する。このとき、サービスプロバイダ 710 は、例えば、著作権情報 705 a, 705 b, 705 c のうち電子透かし情報をコンテンツデータ 704 a, 704 b, 704 c に所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルに SCMS 情報を埋め込む。

さらに、サービスプロバイダ 710 は、コンテンツデータ 707 a, 707 b, 707 c を、鍵データベース 706 から読み出したコンテンツ鍵データ K c a, K c b, K c c を用いてそれぞれ暗号化する。その後、サービスプロバイダ 710 は、暗号化されたコンテンツデータ 707 a, 707 b, 707 c を格納したセキュアコンテナ 722 を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置 709 に存在する CA (Conditional Access) モジュール 711 に送信する。

【0005】

CA モジュール 711 は、セキュアコンテナ 722 をセッション鍵データを用

いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。

この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】

サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益配分を行う。

このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】

また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに

基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】

ところで、SCMSは、CD(Compact Disc)からDAT(Digital Audio Tape)への録音を防止するために規定されたものであり、DATとDATとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダを特定するに止まり、違法なコピーを技術的に阻止するものではない。

従って、上述した図67に示すEMDシステム700では、コンテンツプロバイダの権利(利益)が十分に保護されないという問題がある。

【0009】

また、上述したEMDシステム700では、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

【0010】

また、上述したEMDシステム700では、ユーザの端末装置709からの課金情報721を、サービスプロバイダ710の権利処理モジュール720で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうか懸念される。

【0011】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者(関係者)の利益を適切に保護できるデータ提供システム、その方法および管理装置を提供することを目的とする。

また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の

負担を軽減できるデータ提供システム、その方法および管理装置を提供することを目的とする。

【0012】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第1の観点のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

このとき、前記管理装置による前記権利書データの正当性の証明は、例えば、権利書データに対しての前記管理装置の署名データを作成することによって行われる。

【0013】

本発明の第1の観点のデータ提供システムでは、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

【0014】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

【0015】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

【0016】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

【0017】

また、本発明の第2の観点のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前

記コンテンツ鍵データの正当性を証明する。

【0018】

本発明の第2の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給する。

次に、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

【0019】

また、本発明の第3の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

【0020】

本発明の第3の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給する。

次に、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コ

ンテンツ鍵データの正当性を証明する。

【 0 0 2 1 】

また、本発明の第 4 の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

【 0 0 2 2 】

本発明の第 4 の観点のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供する。

次に、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

【 0 0 2 3 】

また、本発明の第 1 の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用

を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

【 0 0 2 4 】

また、本発明の第 2 の観点の管理装置は、コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該コンテンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータを前記コンテンツ鍵データを用いて復号した後、当該コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

【 0 0 2 5 】

また、本発明の第 3 の観点の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

【 0 0 2 6 】

また、本発明の第 1 の観点のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

【 0 0 2 7 】

また、本発明の第 2 の観点のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデー

タを配給し、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

【0028】

また、本発明の第3の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において、前記権利書データの正当性を証明する。

【0029】

また、本発明の第4の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

【0030】

【0031】

【発明の実施の形態】

以下、本発明の実施形態に係わる EMD (Electronic Music Distribution: 電

子音楽配信) システムについて説明する。

第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。

本実施形態において、ユーザに配信されるコンテンツ(Content) データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102、SAM105₁~105₄などが、それぞれ請求項1に係わるデータ提供装置、管理装置およびデータ処理装置に対応している。

まず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ102に送信する。権利書データ106は、EMDサービスセンタ102によって権威化(認証)される。

【0032】

また、コンテンツプロバイダ101は、コンテンツ鍵データK_cでコンテンツデータCを暗号化してコンテンツファイルCFを生成すると共に、コンテンツ鍵データK_cをEMDサービスセンタ102から配給された対応する期間の配信用鍵データKD₁~KD₅₆で暗号化する。そして、コンテンツプロバイダ101は、暗号化されたコンテンツ鍵データK_cおよびコンテンツファイルCFと自らの署名データとを格納したセキュアコンテナ(モジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク103に配給する。

【0033】

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁ およ

びAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module) 105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers) 1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0034】

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテンツ104、および/または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテンツ104に対応する期間の配信用鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテンツ104は、ネットワーク機器160₁およびAV機器160₂～160₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM105₁～105₄は、上述したセキュアコンテンツ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録する。

利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0035】

EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0036】

本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての（ルート認証局92の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM105₁～105₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化すること、EMDサービスセンタ102の認証機能の一つである。

また、EMDサービスセンタ102は、例えば、配信用鍵データKD₁～KD₆などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price)とSAM105₁～SAM105₄から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理（利益分配）機能を有する。

【0037】

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

〔コンテンツプロバイダ101〕

図2は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM105₁～105₄との間で送受信されるデータに関連するデータの流れが示されている。

また、図3には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。

なお、図3以降の図面では、署名データ処理部、および、セッション鍵データ K_{SES} を用いた暗号化・復号部に入出力するデータの流れは省略している。

【0038】

図2および図3に示すように、コンテンツプロバイダ101は、コンテンツマスターソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、SAM管理部124およびEMDサービスセンタ管理部125を有する。

コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでEMDサービスセンタ102に登録し、自らの識別子（識別番号）CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受ける。

以下、図2および図3に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

【0039】

コンテンツマスターソースサーバ111は、ユーザホームネットワーク103に提供するコンテンツのマスターソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

【0040】

電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wcおよびユーザ電子透かし情報(User Watermark)Wuなどを埋め込んでコンテンツデータS112を生成し、コンテンツデータS112を圧縮部113に出力する。

【0041】

ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコー

ド、オーサリング日付、オーサリング機器ID (Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM105₁～105₄の識別子SAM_ID₁～SAM_ID₄が含まれる。

また、電子透かし情報付加部112は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のIDを電子透かし情報としてコンテンツデータS111に埋め込む。

本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、EMDサービスセンタ102において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0042】

圧縮部113は、コンテンツデータS112を、例えば、ATRAC3 (Adaptive Transform Acoustic Coding 3) (商標)などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

【0043】

暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES (Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。

また、暗号化部 114 は、コンテンツ鍵データ K_c を共通鍵として用い、A/V 伸長用ソフトウェア *Soft* およびメタデータ *Meta* を暗号化した後に、セキュアコンテナ作成部 117 に出力する。

【0044】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号化方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。DES の全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0045】

まず、平文の 64 ビットは、上位 32 ビットの H_0 と下位 32 ビットの L_0 とに分割される。鍵処理部から供給された 48 ビットの拡大鍵データ K_1 および下位 32 ビットの L_0 を入力とし、下位 32 ビットの L_0 を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H_0 と、F 関数の出力との排他的論理和が算出され、その結果は L_1 とされる。また、 L_0 は、 H_1 とされる。

そして、上位 32 ビットの H_0 および下位 32 ビットの L_0 を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの H_{16} および下位 32 ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【0046】

乱数発生部 115 は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データ K_c として暗号化部 114 および暗号化部 116 に出力する。

なお、コンテンツ鍵データ K_c は、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データ K_c は、例えば、所定時間毎に更新される。

【0047】

暗号化部 116 は、後述するようにして EMD サービスセンタ 102 から受信されて記憶部 119 に記憶された配信用鍵データ $KD_1 \sim KD_6$ のうち対応する期間の配信用鍵データ $KD_1 \sim KD_6$ を入力し、当該配信用鍵データを共通鍵として用いた DES などの共通暗号化方式によって図 4 (B) に示すコンテンツ鍵データ Kc 、権利書データ 106、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ および署名・証明書モジュール Mod_1 を暗号化した後に、セキュアコンテナ作成部 117 に出力する。

署名・証明書モジュール Mod_1 には、図 4 (B) に示すように、署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ 、コンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} および当該公開鍵証明書 CER_{CP} に対しての EMD サービスセンタ 102 の署名データ $SIG_{1,ESC}$ が格納されている。

また、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ は、SAM 105₁ \sim 105₄ 内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ (UCP) U106 のシンタックス (文法) を示す $UCP-L$ (Label) . R (Reader) と、SAM 105₁ \sim 105₄ に内蔵された記憶部 (フラッシュ ROM) の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データとを格納している。

【0048】

なお、記憶部 119 は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データ $KD_1 \sim KD_6$ を記憶するデータベースおよびキーファイル KF を記憶するデータベースなどの種々のデータベースを備えている。

【0049】

署名処理部 117 は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ 101 の秘密鍵データ $K_{CP,S}$ を用いて、その署名データ SIG を作成する。

【0050】

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧

縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0051】

セキュアコンテナ作成部118は、図4（A）に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたコンテンツデータC、A/V伸長用ソフトウェアSoftおよびメタデータMetaとを格納したコンテンツファイルCFを生成する。

ここで、A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器160₁ およびAV機器160₂ ~160₄ において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。

【0052】

また、セキュアコンテナ作成部118は、図4（B）に示すように、暗号化部116から入力した対応する期間の配信用鍵データKD₁ ~KD₆ で暗号化されたコンテンツ鍵データKc、権利書データ（UCP）106およびSAMプログラム・ダウンロード・コンテナSDC₁ ~SDC₃ および署名・証明書モジュールMod₁ を格納したキーファイルKFを生成する。

そして、セキュアコンテナ作成部118は、図4（A）、（B）に示すコンテンツファイルCFおよびキーファイルKFと、図4（C）に示すコンテンツプロバイダ101の公開鍵データK_{CP}および署名データSIG_{1,ESC} とを格納したセキュアコンテナ104を生成し、これをセキュアコンテナデータベース118aに格納した後に、ユーザからの要求に応じてSAM管理部124に出力する。

このように、本実施形態では、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}をセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band) 方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CER_{CP}を得るための通信をEMDサービスセンタ102との間で行う必要がない。

なお、本発明では、公開鍵証明書 $CE R_{CP}$ をセキュアコンテナ 104 に格納しないで、ユーザホームネットワーク 103 が EMD サービスセンタ 102 から公開鍵証明書 $CE R_{CP}$ を得るアウト・オブ・バンド (Out-Of-band) 方式を採用してもよい。

【0053】

相互認証部 120 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 との間でオンラインでデータを送受信する際に、それぞれ EMD サービスセンタ 102 およびユーザホームネットワーク 103 との間で相互認証を行ってセッション鍵データ (共有鍵) K_{SES} を生成する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0054】

暗号化・復号部 121 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 にオンラインで送信するデータを、セッション鍵データ K_{SES} を用いて暗号化する。

また、暗号化・復号部 121 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 からオンラインで受信したデータを、セッション鍵データ K_{SES} を用いて復号する。

【0055】

権利書データ作成部 122 は、権利書データ 106 を作成し、これを暗号化部 116 に出力する。

権利書データ 106 は、コンテンツデータ C の運用ルールを定義した記述子 (ディスクリプター) であり、例えば、コンテンツプロバイダ 101 の運用者が希望する標準小売価格 SRP (Suggested Retailer' Price) やコンテンツデータ C の複製ルールなどが記述されている。

【0056】

SAM 管理部 124 は、セキュアコンテナ 104 を、オフラインおよび／またはオンラインでユーザホームネットワーク 103 に供給する。

SAM 管理部 124 は、CD-ROM や DVD などの ROM 型の記録媒体 (メディア) を用いてセキュアコンテナ 104 をオフラインでユーザホームネットワ

ーク 103 に配給する場合には、配信用鍵データ $KD_1 \sim KD_6$ などを用いてセキュアコンテナ 104 を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク 103 にオフラインで供給される。

【0057】

図 5 は、ROM 型の記録媒体 130 を説明するための図である。

図 5 に示すように、ROM 型の記録媒体 130 は、ROM 領域 131、RAM 領域 132 およびメディア SAM 133 を有する。

ROM 領域 131 には、図 4 (A) に示したコンテンツファイル CF が記憶されている。

また、RAM 領域 132 には、図 4 (B)、(C) に示したキーファイル KF および公開鍵証明書データ CER_{CP} と機器の種類に応じて固有の値を持つ記録用鍵データ K_{STR} とを引数として MAC 関数を用いて生成したと署名データと、当該キーファイル KF および公開鍵証明書データ CER_{CP} とを記録媒体に固有の値を持つメディア鍵データ K_{MED} を用いて暗号化したデータとが記憶される。

また、RAM 領域 132 には、例えば、不正行為などで無効となったコンテンツプロバイダ 101 および $SAM105_1 \sim 105_5$ を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

また、また、RAM 領域 132 には、後述するようにユーザホームネットワーク 103 の $SAM105_1 \sim 105_4$ においてコンテンツデータ C の購入・利用形態が決定されたときに生成される利用制御状態（UCS）データ 166 などが記憶される。これにより、利用制御状態データ 166 が RAM 領域 132 に記憶されることで、購入・利用形態が決定した ROM 型の記録媒体 130 となる。

メディア SAM 133 には、例えば、ROM 型の記録媒体 130 の識別子であるメディア ID と、メディア鍵データ K_{MED} とが記憶されている。

メディア SAM 133 は、例えば、相互認証機能を有している。

【0058】

また、SAM 管理部 124 は、セキュアコンテナ 104 を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク 103 に配信す

る場合には、暗号化・復号部 121 においてセッション鍵データ K_{SES} を用いてセキュアコンテナ 104 を暗号化した後に、ネットワークを介してユーザホームネットワーク 103 に配信する。

本実施形態では、SAM 管理部、EMD サービスセンタ 管理部、並びに後述するコンテンツプロバイダ 管理部およびサービスプロバイダ 管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0059】

ここで、コンテンツプロバイダ 101 からユーザホームネットワーク 103 へのコンテンツデータ C の配給は、上述したように記録媒体 130 を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ 106 が格納された共通の形式のセキュアコンテナ 104 を用いる。従って、ユーザホームネットワーク 103 の SAM 105₁ ~ 105₄ では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ 106 に基づいた権利処理を行なうことができる。

【0060】

また、上述したように、本実施形態では、セキュアコンテナ 104 内に、コンテンツ鍵データ K_c で暗号化されたコンテンツデータ C と、当該暗号化を解くためのコンテンツ鍵データ K_c とを同封するイン・バンド (In-Band) 方式を採用している。イン・バンド方式では、ユーザホームネットワーク 103 の機器で、コンテンツデータ C を再生しようとするときに、コンテンツ鍵データ K_c を別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データ K_c は配信用鍵データ KD_1 ~ KD_6 で暗号化されているが、配信用鍵データ KD_1 ~ KD_6 は、EMD サービスセンタ 102 で管理されており、ユーザホームネットワーク 103 の SAM 105₁ ~ 105₅ に事前に (SAM 105₁ ~ 105₄ が EMD サービスセンタ 102 に初回にアクセスする際に) 配信されているので、ユーザホームネットワーク 103 では、EMD サービスセンタ 102 との間をオンラインで接続することなく、オフラインで、コンテンツデータ C の利用が可能になる。

なお、本発明は、コンテンツデータCとコンテンツ鍵データK_cとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0061】

EMDサービスセンタ管理部125は、EMDサービスセンタ102から6カ月の配信用鍵データK_{D1}～K_{D6} およびそれぞれに対応した署名データS I G_{KD1,ESC}～S I G_{KD6,ESC} と、コンテンツプロバイダ101の公開鍵データK_{CP,P}を含む公開鍵証明書C E R_{CP}およびその署名データS I G_{1,ESC} と、決済レポートデータ107とを受信すると、これらを暗号化・復号部121においてセッション鍵データK_{SES} を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

【0062】

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique)な識別子C o n t e n t _ I D、公開鍵データK_{CP,P}およびそれらの署名データS I G_{9,CP}を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データK_{CP,P}の公開鍵証明書データC E R_{CP}を入力する。

また、EMDサービスセンタ管理部125は、権利書データ106をEMDサービスセンタ102に登録する際に、図6(A)に示すように、提供するコンテンツデータCのグローバルユニークな識別子C o n t e n t _ I D、コンテンツ鍵データK_cおよび権利書データ106を格納したモジュールM o d₃ と、その署名データS I G_{5,CP}とを格納した権利書登録要求用モジュールM o d₂ を作成し、これを暗号化・復号部121においてセッション鍵データK_{SES} を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。

EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0063】

以下、図2および図3を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶される。

【0064】

先ず、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データ $K_{CP,S}$ に対応する公開鍵データ $K_{CP,S}$ の正当性を証明する公開鍵証明書データ CER_{CP} を要求する場合の処理を図3を参照しながら説明する。

先ず、コンテンツプロバイダ101は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{CP,S}$ を生成し、当該秘密鍵データ $K_{CP,S}$ に対応する公開鍵データ $K_{CP,P}$ を作成して記憶部119に記憶する。

EMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子CP_IDおよび公開鍵データ $K_{CP,P}$ を記憶部119から読み出す。

そして、EMDサービスセンタ管理部125は、識別子CP_IDおよび公開鍵データ $K_{CP,P}$ を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ管理部125は、当該登録に応じて、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ をEMDサービスセンタ102から入力して記憶部119に書き込む。

【0065】

次に、コンテンツプロバイダ101が、EMDサービスセンタ102から配信用鍵データを受信する処理を図3を参照しながら説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101は、EMDサービスセンタ102から既に公開鍵証明書データ CER_{CP} を得ている必要がある。

EMDサービスセンタ管理部125が、EMDサービスセンタ102から6カ

月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ を入力し、これを記憶部 119 内の所定のデータベースに記憶する。

そして、署名処理部 117 において、記憶部 119 に記憶された署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ の正当性が確認された後に、記憶部 119 に記憶されている配信用鍵データ $KD_1 \sim KD_6$ が有効なものとして扱われる。

【0066】

次に、コンテンツプロバイダ 101 がユーザホームネットワーク 103 の $SAM105_1$ にセキュアコンテナ 104 を送信する場合の処理を図 2 を参照しながら説明する。

なお、以下の例では、コンテンツプロバイダ 101 から $SAM105_1$ にセキュアコンテナ 104 を送信する場合を例示するが、セキュアコンテナ 104 を $SAM105_2 \sim 105_4$ に送信する場合も、 $SAM105_1$ を介して $SAM105_2 \sim 105_4$ に送信される点を除いて同じである。

まず、コンテンツデータ $S111$ がコンテンツマスタソースサーバ 111 から読み出されて電子透かし情報付加部 112 に出力される。

次に、電子透かし情報付加部 112 は、コンテンツデータ $S111$ に電子透かし情報を埋め込んでコンテンツデータ $S112$ を生成し、これを圧縮部 113 に出力する。

次に、圧縮部 113 は、コンテンツデータ $S112$ を、例えば $ATRAC3$ 方式で圧縮してコンテンツデータ $S113$ を作成し、これを暗号化部 114 に出力する。

また、乱数発生部 115 から暗号化部 114 に、乱数を発生して生成されたコンテンツ鍵データ Kc が出力される。

【0067】

次に、暗号化部 114 は、コンテンツデータ $S113$ と、記憶部 119 から読み出されたメタデータ $Meta$ および A/V 伸長用ソフトウェア $Soft$ とを、コンテンツ鍵データ Kc を用いて暗号化してセキュアコンテナ作成部 118 に出力する。この場合に、メタデータ $Meta$ は暗号化しなくてもよい。

そして、セキュアコンテナ作成部 118 は、図 4 (A) に示すコンテンツファイル CF を作成する。また、署名処理部 117 において、コンテンツファイル CF のハッシュ値がとられ、秘密鍵データ $K_{CP,S}$ を用いて署名データ $SIG_{6,CP}$ が生成される。

【0068】

また、署名処理部 117 は、コンテンツデータ C、コンテンツ鍵データ K_c および権利書データ 106 のそれぞれに対してハッシュ値をとり、秘密鍵データ $K_{CP,S}$ を用いて、それぞれのデータの作成者（提供者）の正当性を示す署名データ $SIG_{2,CP}$ 、 $SIG_{3,CP}$ 、 $SIG_{4,CP}$ を作成する。

また、暗号化部 116 は、図 4 (B) に示すコンテンツ鍵データ K_c 、権利書データ 106、SAM プログラム・ダウンロード・コンテナ $SD_1 \sim SD_3$ および署名・証明書モジュール Mod_1 を、対応する期間の配信用鍵データ $KD_1 \sim KD_3$ で暗号化してセキュアコンテナ作成部 118 に出力する。

そして、セキュアコンテナ作成部 118 は、図 4 (B) に示すキーファイル KF を作成する。

また、署名処理部 117 は、キーファイル KF のハッシュ値をとり、秘密鍵データ $K_{CP,S}$ を用いて、署名データ $SIG_{7,CP}$ を作成する。

【0069】

次に、セキュアコンテナ作成部 118 は、図 4 (A) に示すコンテンツファイル CF およびその署名データ $SIG_{6,CP}$ と、図 4 (B) に示すキーファイル KF およびその署名データ $SIG_{7,CP}$ と、図 4 (C) に示す公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ とを格納したセキュアコンテナ 104 を作成し、これを、セキュアコンテナデータベース 118a に記憶する。そして、セキュアコンテナ作成部 118 は、例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク 103 に提供しようとするセキュアコンテナ 104 をセキュアコンテナデータベース 118a から読み出して、相互認証部 120 と SAM 105₁ との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化・復号部 121 において暗号化した後に、SAM 管理部 124 を介してユーザホームネットワーク 103 の SAM 105₁ に送信する。

【0070】

次に、コンテンツプロバイダ101が、EMDサービスセンタ102に権利書データ106およびコンテンツ鍵データKcを登録して権威化することを要求する場合の処理を図3を参照して説明する。

権利書データ106およびコンテンツ鍵データKcの権威化要求処理は、個々のコンテンツデータC毎に行われる。

【0071】

この場合には、署名処理部117において、記憶部119から読み出したコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106からなるモジュールMod₃のハッシュ値が求められ、秘密鍵データK_{CP,S}を用いて署名データSIG_{5,CP}が生成される。

そして、図6(A)に示す権利登録要求用モジュールMod₂を、相互認証部120とEMDサービスセンタ102との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部121において暗号化した後に、EMDサービスセンタ管理部125からEMDサービスセンタ102に送信する。

【0072】

本実施形態では、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、コンテンツプロバイダ101がEMDサービスセンタ102から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ101において配信用鍵データKD₁～KD₆を用いて暗号化を行ってキーフファイルKFを作成する場合を例示する。

但し、本発明は、例えば、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、配信用鍵データKD₁～KD₆を用いて暗号化した図6(B)に示す権威化証明書モジュールMod_{2a}を送信してもよい。

権威化証明書モジュールMod_{2a}は、コンテンツデータCのグローバルユニーク

クな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106を格納したモジュールMod_{3a}と、秘密鍵データK_{ESC,S}を用いたモジュールMod_{3a}の署名データSIG_{5a,ESC}とを格納している。

この場合には、コンテンツプロバイダ101は、例えば、セキュアコンテナ104内に、権威化証明書モジュールMod_{2a}を格納してSAM105₁～105₄に配給する。

なお、EMDサービスセンタ102は、それぞれ異なる月に対応する配信用鍵データKD₁～KD₆を用いて暗号化した6カ月分の権威化証明書モジュールMod_{2a}を生成し、これらをまとめてコンテンツプロバイダ101に送信してもよい。

【0073】

〔EMDサービスセンタ102〕

EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing) (利益分配)機能を有する。

図7は、EMDサービスセンタ102の機能の構成図である。

図7に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、CERデータベース145a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150および暗号化・復号部151を有する。

なお、図7には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流れが示されている。

また、図8には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、SAM105₁～105₄および図1に示す決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0074】

鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部148およびSAM管理部149に出力する。

また、鍵データベース141a配信用鍵データKDの他に、記録用鍵データKSTR、メディア鍵データK_{MED} およびMAC鍵データK_{MAC} などの鍵データを記憶する一連の鍵データベースからなる。

【0075】

決算処理部142は、SAM105₁～105₄から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144に出力する。

なお、決算処理部142は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ108は、ユーザホームネットワーク103におけるセキュアコンテナ104の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部142においてセキュアコンテナ104に関連したライセンス料の支払い額を決定する際に用いられる。

【0076】

利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105₁～105₄の識別子SAM_ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記

録媒体などのライセンス所有者に、ユーザホームネットワーク 103 のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ 107 および決済請求権データ 152 を作成する。当該分配率表は、例えば、セキュアコンテンツ 104 に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ 152 は、当該データに基づいて、決済機関 91 に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関 91 は、決済が終了すると、当該決済機関の利用明細書を EMD サービスセンタ 102 に送る。EMD サービスセンタ 102 は、当該利用明細書の内容を、対応する権利者に通知する。

【0077】

決算機関管理部 144 は、決算処理部 142 が生成した決済請求権データ 152 を図 1 に示すペイメントゲートウェイ 90 を介して決済機関 91 に送信する。

なお、後述するように、決算機関管理部 144 は、決済請求権データ 152 を、コンテンツプロバイダ 101 などの権利者に送信し、権利者自らが、受信した決済請求権データ 152 を用いて決済機関 91 に決済を行ってもよい。

また、決算機関管理部 144 は、署名処理部 143 において決済請求権データ 152 のハッシュ値をとり、秘密鍵データ $K_{ESC,S}$ を用いて生成した署名データ SIG_{gg} を決済請求権データ 152 と共に決済機関 91 に送信する。

【0078】

証明書・権利書管理部 145 は、CER データベース 145a に登録されて権威化された公開鍵証明書データ CER_{CP} および公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ などを読み出すと共に、コンテンツプロバイダ 101 の権利書データ 106 およびコンテンツ鍵データ K_c などを CER データベース 145a に登録して権威化する。

なお、公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を格納するデータースと、権利書データ 106 およびコンテンツ鍵データ K_c とを個別に設けてもよい。

このとき、証明書・権利書管理部 145 は、例えば、権利書データ 106 およびコンテンツ鍵データ K_c などのハッシュ値をとり、秘密鍵データ $K_{ESC,S}$ を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

【0079】

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されたコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

【0080】

SAM 管理部 149 は、ユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ との間で通信する機能を有し、登録された SAM の識別子 SAM_ID や SAM 登録リストなどを記録した SAM データベース 149a にアクセスできる。

【0081】

以下、 EMD サービスセンタ 102 内での処理の流れを説明する。

まず、 EMD サービスセンタ 102 からコンテンツプロバイダ 101 およびユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ への配信用鍵データを送信する際の処理の流れを、図 7 および図 8 を参照しながら説明する。

図 7 に示すように、鍵サーバ 141 は、所定期間毎に、例えば、6 カ月分の配信用鍵データ $KD_1 \sim KD_6$ を鍵データベース 141a から読み出してコンテンツプロバイダ管理部 148 に出力する。

また、署名処理部 143 は、配信用鍵データ $KD_1 \sim KD_6$ の各々のハッシュ値をとり、 EMD サービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ を用いて、それぞれに対応する署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ を作成し、これをコンテンツプロバイダ管理部 148 に出力する。

コンテンツプロバイダ管理部 148 は、この 6 カ月分の配信用鍵データ $KD_1 \sim KD_6$ およびそれらの署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ を、相互認証部 150 と図 3 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

【0082】

また、図8に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データ $KD_1 \sim KD_3$ を鍵データベース141aから読み出してSAM管理部149に出力する。

また、署名処理部143は、配信用鍵データ $KD_1 \sim KD_3$ の各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いて、それぞれに対応する署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を作成し、これをSAM管理部149に出力する。

SAM管理部149は、この3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびそれらの署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を、相互認証部150とSAM105₁～105₄と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、SAM105₁～105₄に送信する。

【0083】

次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データ CER_{CP} の発行要求を受けた場合の処理を、図7を参照しながら説明する。

この場合に、コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子 CP_ID 、公開鍵データ $K_{CP,P}$ および署名データ $SIG_{9,CP}$ をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_{9,CP}$ の正当性を署名処理部143において確認した後に、識別子 CP_ID および公開鍵データ $K_{CP,P}$ に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。

そして、証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データ CER_{CP} をCERデータベース145aから読み出してコンテンツプロバイダ管理部148に出力する。

また、署名処理部143は、公開鍵証明書データ CER_{CP} のハッシュ値をとり

、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{1,ESC}$ を作成し、これをコンテンツプロバイダ管理部148に出力する。

そして、コンテンツプロバイダ管理部148は、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0084】

次に、EMDサービスセンタ102が $SAM105_1$ から、公開鍵証明書データ CER_{SAM1} の発行要求を受けた場合の処理を、図8を参照しながら説明する。

この場合に、SAM管理部149は、 $SAM105_1$ の識別子 SAM_1-ID 、公開鍵データ $K_{SAM1,P}$ および署名データ $SIG_{8,SAM1}$ を $SAM105_1$ から受信すると、これらを、相互認証部150と $SAM105_1$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_{8,SAM1}$ の正当性を署名処理部143において確認した後に、識別子 SAM_1-ID および公開鍵データ $K_{SAM1,P}$ に基づいて、当該公開鍵証明書データの発行要求を出した $SAM105_1$ がSAMデータベース149aに登録されているか否かを確認する。

そして、証明書・権利書管理部145は、当該 $SAM105_1$ の公開鍵証明書データ CER_{SAM1} をCERデータベース145aから読み出してSAM管理部149に出力する。

た、署名処理部143は、公開鍵証明書データ CER_{SAM1} のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{50,ESC}$ を作成し、これをSAM管理部149に出力する。

そして、SAM管理部149は、公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{50,ESC}$ を、相互認証部150と $SAM105_1$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、 $SAM105_1$ に送信する。

なお、 $SAM105_2 \sim 105_4$ が、公開鍵証明書データを要求した場合の処理は、対象が $SAM105_2 \sim 105_4$ に代わるのみで、基本的に上述したSA

M105₁ の場合と同じである。

なお、本発明では、EMDサービスセンタ102は、例えば、SAM105₁の出荷時に、SAM105₁の秘密鍵データ $K_{SAM1,S}$ および公開鍵データ $K_{SAM1,P}$ をSAM105₁の記憶部に記憶する場合には、当該出荷時に、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データ CER_{SAM1} を、SAM105₁の記憶部に記憶してもよい。

【0085】

次に、EMDサービスセンタ102が、コンテンツプロバイダ101から権利書データ106およびコンテンツ鍵データ K_c の登録要求を受けた場合の処理を、図7を参照しながら説明する。

この場合には、コンテンツプロバイダ管理部148がコンテンツプロバイダ101から図6(A)に示す権利書登録要求モジュール Mod_2 を受信すると、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて権利書登録要求モジュール Mod_2 を復号する。

そして、署名処理部143において、鍵データベース141aから読み出した公開鍵データ K_{cp} を用いて、署名データ $SIG_{5,CP}$ の正当性を検証する。

次に、証明書・権利書管理部145は、権利書登録要求モジュール Mod_2 に格納された権利書データ106およびコンテンツ鍵データ K_c を、 CER データベース145aに登録する。

【0086】

次に、EMDサービスセンタ102において決済処理を行なう場合の処理を図8を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク103の例えばSAM105₁から利用履歴データ108およびその署名データ $SIG_{200,SAM1}$ を入力すると、利用履歴データ108および署名データ $SIG_{200,SAM1}$ を、相互認証部150とSAM105₁との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて復号し、SAM105₁の公開鍵データ K_{SAM1} による署名データ $SIG_{200,SAM1}$ の検証を行なった後に、決算処理部142に出力する。

【0087】

そして、決算処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書・権利書管理部145を介してCERデータベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。

決算処理部142は、決済請求権データ152を決算機関管理部144に出力すると共に、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

【0088】

次に、決算機関管理部144は、決済請求権データ152およびその署名データSIG₉₉を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

【0089】

次に、EMDサービスセンタ102がコンテンツプロバイダ101に決済レポートを送信する場合の処理を図7を参照しながら説明する。

決算処理部142において決済が行なわれると、前述したように、決算処理部142からコンテンツプロバイダ管理部148に決済レポートデータ107が出力される。

決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

EMDサービスセンタ102は、決算処理部142から決済レポートデータ107を入力すると、これを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0090】

また、EMDサービスセンタ102は、前述したように、権利書データ106を登録（権威化）した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、図6（B）に示す権威化証明書モジュールMod_{2a}を配信用鍵データKD₁～KD₆で暗号化して送信してもよい。

【0091】

また、EMDサービスセンタ102は、その他に、SAM105₁～105₄の出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

【0092】

〔ユーザホームネットワーク103〕

ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160₁およびA/V機器160₂～160₄を有している。

ネットワーク機器160₁は、SAM105₁を内蔵している。また、AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。

SAM105₁～105₄の相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器160₂～160₄は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160₁のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク103は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0093】

以下、ネットワーク機器160₁について説明する。

図9は、ネットワーク機器160₁の構成図である。

図9に示すように、ネットワーク機器160₁は、SAM105₁、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を

有する。

【0094】

SAM105₁ ~ 105₄ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。

SAM105₁ ~ 105₄ は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁ ~ 105₄ のIC(Integrated Circuit)の内部の仕様を知ることはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160₁ およびAV機器160₂ ~ 160₄ に搭載される。

【0095】

SAM105₁ ~ 105₄ は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)である。

SAM105₁ ~ 105₄ の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【0096】

以下、SAM105₁ の機能について詳細に説明する。

なお、SAM105₂ ~ 105₄ は、SAM105₁ と基本的に同じ機能を有している。

図10は、SAM105₁ の機能の構成図である。

なお、図10には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図 10 に示すように、SAM105₁ は、相互認証部 170、暗号化・復号部 171、172、173、コンテンツプロバイダ管理部 180、誤り訂正部 181、ダウンロードメモリ管理部 182、セキュアコンテナ復号部 183、復号・伸長モジュール管理部 184、EMD サービスセンタ管理部 185、利用監視部 186、課金処理部 187、署名処理部 189、SAM 管理部 190、メディア SAM 管理部 197、スタック（作業）メモリ 200 および外部メモリ管理部 811 を有する。

なお、AV 機器 160₂ ~ 160₄ はダウンロードメモリ 167 を有していないため、SAM105₂ ~ 105₄ にはダウンロードメモリ管理部 182 は存在しない。

【0097】

なお、図 10 に示す SAM105₁ の所定の機能は、例えば、図示しない CPU において秘密プログラムを実行することによって実現される。

また、スタックメモリ 200 には、以下に示す処理を経て、図 11 に示すように、利用履歴データ 108 および SAM 登録リストが記憶される。

ここで、外部メモリ 201 のメモリ空間は、SAM105₁ の外部（例えば、ホスト CPU 810）からは見ることはできず、SAM105₁ のみが外部メモリ 201 の記憶領域に対してのアクセスを管理できる。

外部メモリ 201 としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、スタックメモリ 200 としては、例えば SARAM が用いられ、図 12 に示すように、セキュアコンテナ 104、コンテンツ鍵データ K_c、権利書データ（UCP）106、記憶部 192 のロック鍵データ K_{LOC}、コンテンツプロバイダ 101 の公開鍵証明書 CER_{CP}、利用制御状態データ（UCS）166、および SAM プログラム・ダウンロード・コンテナ SDC₁ ~ SDC₃ などが記憶される。

【0098】

以下、SAM105₁ の機能のうち、コンテンツプロバイダ 101 からのセキュアコンテナ 104 を入力したときの各機能ブロックの処理内容を図 10 を参照

しながら説明する。

【0099】

相互認証部170は、SAM105₁がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ（共有鍵） K_{SES} を生成し、これを暗号化・復号部171に出力する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0100】

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データ K_{SES} を用いて暗号化・復号する。

【0101】

誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。

なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部181を、SAM105₁に内蔵した場合を例示したが、誤り訂正部181の機能を、例えばホストCPU810などのSAM105₁の外部に持たせてもよい。

【0102】

ダウンロードメモリ管理部182は、図9に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ104を、相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化して図9に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図13に示すように、HDD(Hard Disk Drive)などの相互認証機能を

備えていないメモリをダウンロードメモリ 211 として用いる場合には、ダウンロードメモリ 211 内はセキュアではないので、コンテンツファイル CF をダウンロードメモリ 211 にダウンロードし、機密性の高いキーファイル KF を例えば、図 10 に示すスタックメモリ 200 にダウンロードする。

【0103】

セキュアコンテナ復号部 183 は、ダウンロードメモリ管理部 182 から入力したセキュアコンテナ 104 に格納されたキーファイル KF を、記憶部 192 から読み出した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号し、署名処理部 189 において署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の正当性、すなわちコンテンツデータ C、コンテンツ鍵データ K_c および権利書データ 106 の作成者の正当性を確認した後に、スタックメモリ 200 に書き込む。

【0104】

EMD サービスセンタ管理部 185 は、図 1 に示す EMD サービスセンタ 102 との間の通信を管理する。

【0105】

署名処理部 189 は、記憶部 192 から読み出した EMD サービスセンタ 102 の公開鍵データ $K_{ESC,P}$ およびコンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ を用いて、セキュアコンテナ 104 内の署名データの検証を行なう。

【0106】

記憶部 192 は、 $SAM105_1$ の外部から読み出しおよび書き換えできない秘密データとして、図 14 に示すように、配信用鍵データ $KD_1 \sim KD_3$ 、 SAM_ID 、ユーザ ID、パスワード、情報参照用 ID、SAM 登録リスト、記録用鍵データ K_{STR} 、ルート CA の公開鍵データ $K_{R-CA,P}$ 、EMD サービスセンタ 102 の公開鍵データ $K_{ESC,P}$ 、メディア鍵データ K_{MED} 、EMD サービスセンタ 102 の公開鍵データ $K_{ESC,P}$ 、 $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ 、 $SAM105_1$ の公開鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書 CER_{SAM1} 、EMD サービスセンタ 102 の秘密鍵データ $K_{ESC,S}$ を用いた公開鍵証明書 CER_{ESC} の署名データ SIG_{22} 、復号・伸長モジュール 163 との間の相互認証用の元鍵データ、メディア SAM との間の相互認証用の元鍵データを記憶している。

また、記憶部 192 には、図 10 に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部 192 としては、例えば、フラッシュ-EEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0107】

以下、EMDサービスセンタ 102 から受信した配信用鍵データ $KD_1 \sim KD_3$ を記憶部 192 に格納する際の $SAM105_1$ 内での処理の流れを図 10 を参照しながら説明する。

この場合には、まず、相互認証部 170 と図 7 に示す相互認証部 150 との間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ K_{SES} で暗号化された 3 カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ が、EMDサービスセンタ 102 から EMDサービスセンタ管理部 185 を介してスタックメモリ 811 に書き込まれる。

次に、暗号化・復号部 171 において、セッション鍵データ K_{SES} を用いて、配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ が復号される。

次に、署名処理部 189 において、スタックメモリ 811 に記憶された署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ の正当性が確認された後に、配信用鍵データ $KD_1 \sim KD_3$ が記憶部 192 に書き込まれる。

【0108】

以下、セキュアコンテナ 104 をコンテンツプロバイダ 101 から入力し、セキュアコンテナ 104 内のキーファイル K_F を復号する際の $SAM105_1$ 内での処理の流れを図 10 を参照しながら説明する。

図 10 に示す $SAM105_1$ の相互認証部 170 と図 2 に示す相互認証部 120 との間で相互認証が行なわれる。

暗号化・復号部 171 は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、コンテンツプロバイダ管理部 180 を介してコンテンツプロバイダ 101 から供給されたセキュアコンテナ 104 を復号する。

【0109】

次に、署名処理部189は、図4（C）に示す署名データ $SIG_{1,ESC}$ の検証を行なった後に、図4（C）に示す公開鍵証明書データ CER_{CP} 内に格納されたコンテンツプロバイダ101の公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{6,CP}$ 、 $SIG_{7,CP}$ の正当性を確認する。

コンテンツプロバイダ管理部180は、署名データ $SIG_{6,CP}$ 、 $SIG_{7,CP}$ の正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する。

【0110】

誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ダウンロードメモリ管理部182は、相互認証部170と図9に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104をダウンロードメモリ167に書き込む。

【0111】

次に、ダウンロードメモリ管理部182は、相互認証部170と図9に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図4（B）に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0112】

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFを復号し、図4（B）に示す署名・証明書モジュール Mod_1 に格納された署名データ $SIG_{1,ESC}$ 、 $SIG_{2,CP} \sim SIG_{4,CP}$ を署名処理部189に出力する。

署名処理部189は、図4（B）に示す署名データ $SIG_{1,ESC}$ の検証を行なった後に、図4（B）に示す公開鍵証明書データ CER_{CP} 内に格納された公開鍵データ $K_{ESC,P}$ を用いて署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の検証を行なう。これにより、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の作成者の正当性が検証される。

【0113】

次に、セキュアコンテナ復号部183は、署名データSIG_{2,CP}～SIG_{4,CP}の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0114】

以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図15を参照しながら説明する。

【0115】

利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ106は、図10を用いて説明したように、復号後にスタックメモリ200に記憶された図4(B)に示すキーファイルKF内に格納されている。

また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

【0116】

課金処理部187は、図9に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0117】

また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモ

リ 200 に記憶された図 4 (B) に示すキーファイル K F の権利書データ 106 内に格納されている。

課金処理部 187 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御状態データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0118】

また、課金処理部 187 は、操作信号 S 165 に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態 (UCS: Usage Control Status) データ 166 を生成し、これをスタックメモリ 200 書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 166 には、コンテンツの ID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれた SAM の SAM__ID、購入を行なったユーザの USER__ID などが記述されている。

【0119】

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁ からコンテンツプロバイダ 101 に利用制御状態データ 166 をコンテンツデータ C の購入と同時にリアルタイムに送信し、コンテンツプロバイダ 101 が EMD サービスセンタ 102 に、利用履歴データ 108 を所定の期間内に SAM105₁ に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ 166 が、コンテンツプロバイダ 101 および EMD サービスセンタ 102 の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ 166 をコンテンツプロバイダ 101 にリアルタイ

ムに送信する。

【0120】

EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。

このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データ $K_{SAM1,s}$ を用いて利用履歴データ108の署名データ $SIG_{200,SAM1}$ を作成し、署名データ $SIG_{200,SAM1}$ を利用履歴データ108と共にEMDサービスセンタ102に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0121】

ダウンロードメモリ管理部182は、例えば、図9に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図9に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

【0122】

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュ

ール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データK_cを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0123】

以下、SAM105₁ 内での処理の流れについて説明する。

まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図15を参照しながら説明する。

まず、ユーザによる図9に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部187に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図9に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図9に示す復号部221において復号された後に、復号部222に出力される。

【0124】

また、スタックメモリ200から読み出されたコンテンツ鍵データK_cおよび半開示パラメータデータ199が、図9に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データK_cおよび半開示パラメータデータ199に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データK_cを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

【0125】

そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

そして、課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

そして、スタックメモリ200に格納されているキーファイルKFに、利用制御状態データ166が加えられ、購入形態が決定した後述する図18（B）に示す新たなキーファイルKF₁が生成される。キーファイルKF₁は、スタックメモリ200に記憶される。

図18（B）に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データK_{STR}を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をMAC（Message Authentication Code）鍵データとして用いて生成したMAC値であるMAC₃₀₀が付されている。また、利用制御状態データ166およびMAC₃₀₀からなるモジュールは、メディア鍵データK_{MED}を用いてDESのCBCモードを利用して

暗号化されている。また、当該モジュールには、当該メディア鍵データ K_{MED} をMAC鍵データとして用いて生成したMAC値である MAC_{301} が付されている。

【0126】

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図15を参照しながら説明する。

この場合には、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図9に示す復号・伸長モジュール163に出力される。このとき、図15に示す相互認証部170と、図9に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。

また、スタックメモリ200から読み出されたコンテンツ鍵データ K_c が復号・伸長モジュール163に出力される。

そして、復号・伸長モジュール163の復号部222において、コンテンツ鍵データ K_c を用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

このとき、課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。

利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データ $SIG_{200,SAM1}$ と共にEMDサービスセンタ102に送信される。

【0127】

次に、図16に示すように、例えば、ネットワーク機器160₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFおよびキーファイルKFを、バス191を介して、AV機器160₂のSAM105₂に転送する場合のSAM105₁内での処理の流れを図17を参照しながら説明する。

ユーザは、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所定のコンテンツを AV 機器 160₂ に転送することを指示し、当該操作に応じた操作信号 S165 が、課金処理部 187 に出力される。

これにより、課金処理部 187 は、操作信号 S165 に基づいて、外部メモリ 201 に記憶されている利用履歴データ 108 を更新する。

【0128】

また、ダウンロードメモリ管理部 182 は、ダウンロードメモリ 167 から読み出した図 18 (A) に示すコンテンツファイル CF を SAM 管理部 190 に出力する。

また、スタックメモリ 200 から読み出した図 18 (B) に示すキーファイル KF₁ を、署名処理部 189 および SAM 管理部 190 に出力する。

署名処理部 189 は、スタックメモリ 200 から読み出したキーファイル KF₁ の署名データ SIG_{42,SAM1} を作成し、これを SAM 管理部 190 に出力する。

また、SAM 管理部 190 は、記憶部 192 から、図 18 (C) に示す公開鍵証明書データ CER_{SAM1} およびその署名データ SIG_{22,ESC} を読み出す。

【0129】

また、相互認証部 170 は、SAM105₂ との間で相互認証を行って得たセッション鍵データ K_{SES} を暗号化・復号部 171 に出力する。

SAM 管理部 190 は、図 18 (A), (B), (C) に示すデータからなる新たなセキュアコンテナを購入、暗号化・復号部 171 において、セッション鍵データ K_{SES} を用いて暗号化した後に、図 16 に示す AV 機器 160₂ の SAM105₂ に出力する。

このとき、SAM105₁ と SAM105₂ との間の相互認証と並行して、IEEE1394 シリアルバスであるバス 191 の相互認証が行われる。

【0130】

以下、図 16 に示すように、SAM105₁ から入力したコンテンツファイル CF などを、RAM 型などの記録媒体（メディア）に書き込む際の SAM105₂ 内での処理の流れを、図 19 を参照しながら説明する。

【0131】

この場合には、SAM105₂のSAM管理部190は、図16に示すように、図18(A)に示すコンテンツファイルCFと、図18(B)に示すキーファイルKF₁ およびその署名データSIG_{42,SAM1} と、図18(C)に示す公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とを、ネットワーク機器160₁のSAM105₁から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF₁ およびその署名データSIG_{42,SAM1} と、公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とが、相互認証部170とSAM105₁の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【0132】

次に、セッション鍵データK_{SES}を用いて復号されたキーファイルKF₁ およびその署名データSIG_{42,SAM1} と、公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とが、スタックメモリ200に書き込まれる。

【0133】

次に、署名処理部189は、スタックメモリ200から読み出した署名データSIG_{22,ESC}を、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1,P}を用いて、署名データSIG_{42,SAM1}の正当を確認する。

【0134】

次に、署名データSIG_{42,SAM1}の正当性、すなわちキーファイルKF₁の作成者の正当性が確認されると、図18(B)に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。

なお、当該例では、キーファイルKF₁の作成者と送信元とが同じ場合を述べたが、キーファイルKF₁の作成者と送信元とが異なる場合には、キーファイルKF₁に対して作成者の署名データと送信者と署名データとが作成され、署名処

理部 189 において、双方の署名データの正当性が検証される。

【0135】

そして、暗号化・復号部 173 は、記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いてキーファイル KF_1 を順に暗号化してメディア SAM 管理部 197 に出力する。

なお、メディア鍵データ K_{MED} は、図 17 に示す相互認証部 170 と図 16 に示す RAM 型の記録媒体 250 のメディア SAM 252 との間の相互認証によって記憶部 192 に事前に記憶されている。

【0136】

ここで、記録用鍵データ K_{STR} は、例えば SACD (Super Audio Compact Disk)、DVD (Digital Versatile Disc) 機器、CD-R 機器および MD (Mini Disc) 機器などの種類（当該例では、AV 機器 160₂）に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。なお、SACD と DVD とでは、ディスク媒体の物理的な構造が同じであるため、DVD 機器を用いて SACD の記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ K_{STR} は、このような場合において、不正コピーを防止する役割を果たす。

【0137】

また、メディア鍵データ K_{MED} は、記録媒体（当該例では、RAM 型の記録媒体 250）にユニークなデータである。

メディア鍵データ K_{MED} は、記録媒体（当該例では、図 16 に示す RAM 型の記録媒体 250）側に格納されており、記録媒体のメディア SAM においてメディア鍵データ K_{MED} を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ K_{MED} は、記録媒体にメディア SAM が搭載されている場合には、当該メディア SAM 内に記憶されており、記録媒体にメディア SAM が搭載されていない場合には、例えば、RAM 領域内のホスト CPU 810 の管理外の領域に記憶されている。

なお、本実施形態のように、機器側の SAM（当該例では、SAM 105₂）とメディア SAM（当該例では、メディア SAM 252）との間で相互認証を行

い、セキュアな通信経路を介してメディア鍵データ K_{MED} を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データ K_{MED} を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データ K_{STR} およびメディア鍵データ K_{MED} が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0138】

また、購入者鍵データ K_{PIN} は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データ K_{PIN} は、EMDサービスセンタ102において管理される。

【0139】

メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイル KF_1 を、図16に示す記録モジュール260に出力する。

そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイル KF_1 を、図16に示すRAM型の記録媒体250のRAM領域251に書き込む。この場合に、キーファイル KF_1 を、メディアSAM252内に書き込むようにしてもよい。

【0140】

次に、コンテンツの購入形態が未決定の図5に示すROM型の記録媒体130をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器160₂において購入形態を決定する際の処理の流れを図20および図21を参照しながら説明する。

AV機器160₂のSAM105₂は、先ず、図21に示す相互認証部170と図5に示すROM型の記録媒体130のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データ K_{MED} を入力する。

なお、SAM105₂が、事前にメディア鍵データ K_{MED} を保持している場合には、当該入力を行わなくても良い。

次に、ROM型の記録媒体130のRAM領域132に記録されているセキュアコンテナ104に格納された図4(B), (C)に示すキーファイルKFおよびその署名データSIG_{7,CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを、メディアSAM管理部197を介して入力し、これをスタックメモリ200に書き込む。

【0141】

次に、署名処理部189において、署名データSIG_{1,ESC}の正当性を確認した後、公開鍵証明書データCER_{CP}から公開鍵データK_{CP,P}を取り出し、この公開鍵データK_{CP,P}を用いて、署名データSIG_{7,CP}の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0142】

署名処理部189において署名データSIG_{7,CP}の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

次に、セキュアコンテナ復号部183において、対応する期間の配信用鍵データKD₁ ~ KD₃を用いて、キーファイルKFを復号する。

次に、署名処理部189において、公開鍵データK_{ESC,P}を用いて、キーファイルKFに格納された署名データSIG_{1,ESCM}の正当性を確認した後、キーファイルKF内の公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、署名データSIG_{2,CP} ~ SIG_{4,CP}の正当性、すなわちコンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106の作成者の正当性を検証する。

【0143】

次に、図21に示す相互認証部170と図20に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM105₂の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データK_cおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体130のROM領域131から読み出したコンテンツデータCを図20に示す復号・伸長モジュール163に出力する。次に、復号・伸長モ

ジュール 163 において、コンテンツデータ C がコンテンツ鍵データ K_c を用いて半開示モードで復号された後に伸長され、再生モジュール 270 に出力される。そして、再生モジュール 270 において、復号・伸長モジュール 163 からのコンテンツデータ C が再生される。

【0144】

次に、ユーザによる図 20 に示す購入形態決定操作部 165 の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号 S165 が課金処理部 187 に入力される。

【0145】

次に、課金処理部 187 は、操作信号 S165 に応じた利用制御状態データ 166 を作成し、これをスタックメモリ 200 に書き込む。

次に、スタックメモリ 200 から暗号化・復号部 173 に、例えば、図 4 (B) に示すキーファイル K_F に利用制御状態データ 166 を格納した図 18 (B) に示す新たなキーファイル K_{F1} が出力される。

【0146】

次に、暗号化・復号部 173 は、スタックメモリ 200 から読み出した図 18 (B) に示すキーファイル K_{F1} を、記憶部 192 から読み出した記録用鍵データ K_{STR}、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いて順次に暗号化してメディア SAM 管理部 197 に出力する。

次に、図 21 に示す相互認証部 170 と図 20 に示すメディア SAM 133 との間で相互認証を行った後に、SAM 管理部 197 は、暗号化・復号部 173 から入力したキーファイル K_{F1} を図 20 に示す記録モジュール 271 を介して ROM 型の記録媒体 130 の RAM 領域 132 あるいはメディア SAM 133 内に書き込む。

これにより、購入形態が決定された ROM 型の記録媒体 130 が得られる。

このとき、課金処理部 187 が生成した利用制御状態データ 166 および利用履歴データ 108 は、所定のタイミングで、スタックメモリ 200 および外部メモリ 201 からそれぞれ読み出しされた EMD サービスセンタ 102 に送信される。

【0147】

以下、図22に示すように、AV機器160₃において購入形態が未決定のROM型の記録媒体130からセキュアコンテナ104を読み出してAV機器160₂に転送し、AV機器160₂において購入形態を決定してRAM型の記録媒体250に書き込む際の処理の流れを説明する。

なお、ROM型の記録媒体130からRAM型の記録媒体250へのセキュアコンテナ104の転送は、図1に示すネットワーク機器160₁およびAV機器160₁～160₄のいずれの間で行ってもよい。

【0148】

まず、AV機器160₃のSAM105₃とROM型の記録媒体130のメディアSAM133との間で相互認証を行い、ROM型の記録媒体130のメディア鍵データK_{MED1}をSAM105₃に転送する。

また、AV機器160₂のSAM105₂とRAM型の記録媒体250のメディアSAM252との間で相互認証を行い、RAM型の記録媒体250のメディア鍵データK_{MED2}をSAM105₂に転送する。

【0149】

次に、SAM105₃は、ROM型の記録媒体130のROM領域131から読み出した図4(A)に示すコンテンツファイルCFと、RAM領域132から読み出した図4(B)，(C)キーファイルKF、署名データSIG_{7,CP}、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを、図23に示す暗号化・復号部172において、対応する期間の配信用鍵データKD₁～KD₃を用いて順に復号する。

次に、暗号化・復号部172で復号されたコンテンツファイルCFは、暗号化・復号部171に出力され、SAM105₃と105₂との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化された後に、SAM管理部190に出力される。

また、暗号化・復号部172で復号されたキーファイルKFは、暗号化・復号部171および署名処理部189に出力される。

署名処理部189は、SAM105₃の秘密鍵データK_{SAM3,S}を用いて、キー

ファイルKFの署名データSIG_{350,SAM3}を作成し、これを暗号化・復号部171に出力する。

【0150】

また、暗号化・復号部171は、記憶部192から読み出したSAM105₃の公開鍵証明書データCER_{SAM3}およびその署名データSIG_{351,ESC}と、キーファイルKFおよびその署名データSIG_{350,SAM3}と、暗号化・復号部172から入力したコンテンツファイルCFとを、SAM105₃と105₂との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM管理部190を介して、AV機器160₂のSAM105₂に出力する。

【0151】

SAM105₂では、図24に示すように、SAM管理部190を介してSAM105₃から入力されたコンテンツファイルCFが、暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号された後に、メディアSAM管理部197を介してRAM型の記録媒体250のRAM領域251に書き込まれる。

【0152】

また、SAM管理部190を介してSAM105₃から入力されたキーファイルKFおよびその署名データSIG_{350,SAM3}と、公開鍵証明書データCER_{SAM3}およびその署名データSIG_{351,ESC}とが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号される。

次に、当該復号された署名データSIG_{351,ESC}が、署名処理部189において署名検証され、その正当性が確認されると、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}を用いて、署名データSIG_{350,SAM3}の正当性、すなわちキーファイルKFの送信元の正当性が確認される。

そして、署名データSIG_{350,SAM3}の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

【0153】

次に、セキュアコンテナ復号部 183 は、対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイル KF を復号し、所定の署名検証を経た後に、当該復号したキーファイル KF をスタックメモリ 200 に書き込む。

【0154】

次に、スタックメモリ 200 に記憶されている既に復号されたキーファイル KF に格納された権利書データ 106 が、利用監視部 186 に出力される。利用監視部 186 は、権利書データ 106 に基づいて、コンテンツの購入形態および利用形態が管理される。

【0155】

次に、例えば、ユーザによって試聴モードが選択されると、既にセッション鍵データ K_{SES} で復号されたコンテンツファイル CF のコンテンツデータ C と、スタックメモリ 200 に記憶されたコンテンツ鍵データ K_c 、権利書データ 106 から得られた半開示パラメータデータ 199 およびユーザ電子透かし情報用データ 196 とが、相互認証を経た後に、図 22 に示す復号・伸長モジュール管理部 184 を介して再生モジュール 270 に出力される。そして、再生モジュール 270 において、試聴モードに対応したコンテンツデータ C の再生が行われる。

【0156】

次に、ユーザによる図 22 に示す購入・利用形態決定操作部 165 の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号 $S165$ が、課金処理部 187 に出力される。

そして、課金処理部 187 において、決定された購入・利用形態に応じて利用制御状態データ 166 および利用履歴データ 108 が生成され、これがスタックメモリ 200 および外部メモリ 201 にそれぞれ書き込まれる。

次に、利用制御状態データ 166 を格納した例えば図 18 (B) に示すキーファイル KF_1 が、スタックメモリ 200 から暗号化・復号部 173 に読み出され、暗号化・復号部 173 において記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED2} および購入者鍵データ K_{PIN} を用いて順に暗号化され、メディア SAM 管理部 197 に出力される。キーファイル KF_1 は、図 2

2に示す記録モジュール271によってRAM型の記録媒体250のRAM領域251あるいはメディアSAM252に書き込まれる。

また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

【0157】

以下、SAM105₁～105₄の実現方法について説明する。

SAM105₁～105₄の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図10に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0158】

例えば、図10に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。

また、図10に示す記憶部192や、図10に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁～105₄に内蔵されるメモリとして、強誘電体メモリー（FeRAM）を用いてもよい。

また、SAM105₁～105₄には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0159】

上述したように、SAM105₁～105₄は、プログラムモジュールや、デ

ータおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM 105₁ ~ 105₄ を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU (Memory Magagement Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM 105₁ ~ 105₄ は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM 105₁ ~ 105₄ 自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0160】

SAM 105₁ ~ 105₄ の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切

りを行う)、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ(MiniOS)と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0161】

次に、図9に示す復号・伸長モジュール163について説明する。

図9に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。

相互認証部220は、復号・伸長モジュール163がSAM105₁からデータを入力する際に、図16に示す相互認証部170との間で相互認証を行ってセッション鍵データK_{SES}を生成する。

【0162】

復号部221は、SAM105₁から入力したコンテンツ鍵データK_c、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データK_{SES}を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データK_cおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0163】

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データK_cを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0164】

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。

伸長部223は、例えば、図4(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0165】

電子透かし情報処理部 224 は、復号されたユーザ電子透かし情報用データ 196 に応じたユーザ電子透かし情報を、復号されたコンテンツデータ C に埋め込み、新たなコンテンツデータ C を生成する。電子透かし情報処理部 224 は、当該新たなコンテンツデータ C を再生モジュール 169 に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータ C を再生するとき、復号・伸長モジュール 163 において埋め込まれる。

なお、本発明では、コンテンツデータ C にユーザ電子透かし情報用データ 196 を埋め込まないようにしてもよい。

【0166】

半開示処理部 225 は、半開示パラメータデータ 199 に基づいて、例えば、コンテンツデータ C のうち復号を行わないブロックと、復号を行うブロックとを復号部 222 に指示する。

また、半開示処理部 225 は、その他に、半開示パラメータデータ 199 に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【0167】

再生モジュール 169 は、復号および伸長されたコンテンツデータ C に応じた再生を行う。

【0168】

次に、コンテンツプロバイダ 101、EMD サービスセンタ 102 およびユーザホームネットワーク 103 の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図 25 (A) は、コンテンツプロバイダ 101 から SAM105₁ にデータ Data をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ 101 から SAM105₁ に、コンテンツプロバイダ 101 と SAM105₁ との間の相互認証によって得たセッション

鍵データ K_{SES} で暗号化したモジュール Mod_{50} が送信される。

モジュール Mod_{50} には、モジュール Mod_{51} およびその秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} が格納されている。

モジュール Mod_{51} には、コンテンツプロバイダ 101 の秘密鍵データ $K_{CP,P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

このように、公開鍵証明書データ CER_{CP} を格納したモジュール Mod_{50} を、コンテンツプロバイダ 101 から $SAM105_1$ に送信することで、 $SAM105_1$ において署名データ SIG_{CP} の検証を行なう際に、EMD サービスセンタ 102 から $SAM105_1$ に公開鍵証明書データ CER_{CP} を送信する必要がなくなる。

【0169】

図 25 (B), (C) は、コンテンツプロバイダ 101 から $SAM105_1$ にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ 101 から $SAM105_1$ に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 25 (B) に示すモジュール Mod_{52} が送信される。

モジュール Mod_{52} には、送信するデータ $Data$ と、その秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} とが格納されている。

また、EMD サービスセンタ 102 から $SAM105_1$ には、EMD サービスセンタ 102 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 25 (C) に示すモジュール Mod_{53} が送信される。

モジュール Mod_{53} には、コンテンツプロバイダ 101 の公開鍵証明書データ CER_{CP} と、その秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} とが格納されている。

【0170】

図25 (D) は、 $SAM105_1$ からコンテンツプロバイダ101にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ101に、コンテンツプロバイダ101と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{54} が送信される。

モジュール Mod_{54} には、モジュール Mod_{55} およびその秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} が格納されている。

モジュール Mod_{55} には、 $SAM105_1$ の秘密鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

このように、公開鍵証明書データ CER_{SAM1} を格納したモジュール Mod_{55} を、 $SAM105_1$ からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データ SIG_{SAM1} の検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データ CER_{SAM1} を送信する必要がなくなる。

【0171】

図25 (E), (F) は、 $SAM105_1$ からコンテンツプロバイダ101にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ101に、コンテンツプロバイダ101と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図25 (E) に示すモジュール Mod_{56} が送信される。

モジュール Mod_{56} には、送信するデータ $Data$ と、その秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} とが格納されている。

また、EMDサービスセンタ102からコンテンツプロバイダ101には、E

MDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図25(F)に示すモジュール Mod_{57} が送信される。

モジュール Mod_{57} には、 $SAM105_1$ の公開鍵証明書データ CER_{SAM1} と、その秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} とが格納されている。

【0172】

図26(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{58} が送信される。

モジュール Mod_{58} には、モジュール Mod_{59} およびその秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} が格納されている。

モジュール Mod_{59} には、コンテンツプロバイダ101の秘密鍵データ $K_{CP,P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対する秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

【0173】

図26(H)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図26(H)に示すモジュール Mod_{60} が送信される。

モジュール Mod_{60} には、送信するデータ $Data$ と、その秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} とが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データ CER_{CP} は既に登録されている。

【0174】

図26(I)は、 $SAM105_1$ からEMDサービスセンタ102にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からEMDサービスセンタ102に、EMDサービスセンタ102と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{61} が送信される。

モジュール Mod_{61} には、モジュール Mod_{62} およびその秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} が格納されている。

モジュール Mod_{62} には、 $SAM105_1$ の秘密鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

【0175】

図26(J)は、 $SAM105_1$ からEMDサービスセンタ102にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からEMDサービスセンタ102に、EMDサービスセンタ102と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図26(J)に示すモジュール Mod_{63} が送信される。

モジュール Mod_{63} には、送信するデータ $Data$ と、その秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} とが格納されている。

このとき、EMDサービスセンタ102には $SAM105_1$ の公開鍵証明書データ CER_{SAM1} は既に登録されている。

以下、SAM105₁ ~ 105₄ の出荷時におけるEMDサービスセンタ102への登録処理について説明する。

なお、SAM105₁ ~ 105₄ の登録処理は同じであるため、以下、SAM105₁ の登録処理について述べる。

SAM105₁ の出荷時には、図8に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図10などに示す記憶部192に以下に示す鍵データが初期登録される。

また、SAM105₁ には、例えば、出荷時に、記憶部192などに、SAM105₁ がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部192には、例えば、図14において左側に「*」が付されているSAM105₁ の識別子SAM_ID、記録用鍵データK_{STR}、ルート認証局2の公開鍵データK_{R-CA}、EMDサービスセンタ102の公開鍵データK_{ESC,P}、SAM105₁ の秘密鍵データK_{SAM1,S}、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22,ESC}、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データCER_{SAM1}は、SAM105₁ を出荷後に登録する際にEMDサービスセンタ102からSAM105₁ に送信してもよい。

【0176】

ここで、ルート認証局2の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データK_{R-CA}は、図1に示すルート認証局2によって発行される。

また、EMDサービスセンタ102の公開鍵データK_{ESC,P}は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データK_{ESC,P}は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データK_{ESC,P}を登録する。

また、ルート認証局 92 は、公開鍵データ $K_{ESC,P}$ の公開鍵証明書データ CER_{ESC} を作成する。公開鍵データ $K_{ESC,P}$ を格納した公開鍵証明書データ CER_{ESC} は、好ましく、 $SAM105_1$ の出荷時に記憶部 192 に記憶される。この場合に、公開鍵証明書データ CER_{ESC} は、ルート認証局 92 の秘密鍵データ $K_{ROOT,S}$ で署名されている。

【0177】

EMD サービスセンタ 102 は、乱数を発生して $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1,P}$ を生成する。

また、EMD サービスセンタ 102 は、ルート認証局 92 の認証をもらって、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{ESC,S}$ を用いて署名データを添付する。すなわち、EMD サービスセンタ 102 は、セカンド CA（認証局）として機能を果たす。

【0178】

また、 $SAM105_1$ には、図 8 に示す EMD サービスセンタ 102 の SAM 管理部 149 により、EMD サービスセンタ 102 の管理下にある一意（ユニーク）な識別子 SAM_ID が割り当てられ、これが $SAM105_1$ の記憶部 192 に格納されると共に、図 8 に示す SAM データベース 149a にも格納され、EMD サービスセンタ 102 によって管理される。

【0179】

また、 $SAM105_1$ は、出荷後、例えば、ユーザによって EMD サービスセンタ 102 と接続され、登録手続を行うと共に、EMD サービスセンタ 102 から記憶部 192 に配信用鍵データ $KD_1 \sim KD_3$ が転送される。

すなわち、 $SAM105_1$ を利用するユーザは、コンテンツをダウンロードする前に EMD サービスセンタ 102 に登録手続が必要である。この登録手続は、例えば、 $SAM105_1$ を搭載している機器（当該例では、ネットワーク機器 160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

$SAM105_1$ は、上述した登録手続を経た後でないと使用できない。

【0180】

EMDサービスセンタ102は、SAM105₁のユーザによる登録手続きに応じて、ユーザに固有の識別子USER_IDを発行し、例えば、図8に示すSAMデータベース149aにおいて、SAM_IDとUSER_IDとの対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、SAM105₁のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行ったり、オフラインで本人の確認を行なう。

【0181】

次に、図14に示すように、SAM105₁内の記憶部192にSAM登録リストを格納する手順について説明する。

図1に示すSAM105₁は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM105₂～SAM105₄のSAM登録リストを得る。

なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図27に示すように、バス191にSAM105₁～105₄に加えてAV機器160₅、160₆のSCMS処理回路105₅、105₆が接続されている場合に、SAM105₁～105₄およびSCMS処理回路105₅、105₆を対象として生成される。

従って、SAM105₁は、当該トポロジーマップから、SAM105₁～105₄についての情報を抽出してSAM登録リストを生成する。

【0182】

SAM登録リストのデータフォーマットは、例えば、図28に示される。

そして、SAM105₁ は、当該SAM登録リストを、EMDサービスセンタ102に登録して署名を得る。

これらの処理は、バス191のセッションを利用してSAM105₁ が自動的に
に行い、EMDサービスセンタ102にSAM登録リストの登録命令を発行する
。

EMDサービスセンタ102は、SAM105₁ から図28に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM105₁ より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。

また、EMDサービスセンタ102は、決済時にはSAM105₁ に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。

なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0183】

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。

図29は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データ K_{CP} の公開鍵証明書 CER_{CP} をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、SAM105₁ ~ 105₄ が所定の登録処理を経た後に、SAM105₁ ~ 105₄ の公開鍵データ $K_{SAM1,P}$ ~ $K_{SAM4,P}$ の公開鍵証明書 CER_{CP1} ~ CER_{CP4} をSAM105₁ ~ 105₄ に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の6カ月分の配信用鍵データ $KD_1 \sim KD_6$ をコンテンツプロバイダ101に送信し、3カ月分の配信用鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク103に送信する。

このように、EMDシステム100では、配信用鍵データ $KD_1 \sim KD_3$ を予め $SAM105_1 \sim 105_4$ に配給しているため、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102との間がオフラインの状態でも、 $SAM105_1 \sim 105_4$ においてコンテンツプロバイダ101から配給されたセキュアコンテナ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、 $SAM105_1 \sim 105_4$ からEMDサービスセンタ102に送信される。

【0184】

ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図6(A)に示す権利登録要求モジュール Mod_2 を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データ Kc を登録して権威化する。

【0185】

ステップS3：コンテンツプロバイダ101は、対応する期間の配信用鍵データ $KD_1 \sim KD_6$ などを用いて暗号化を行って、図4(A)，(B)に示すコンテンツファイル CF およびキーファイル KF を作成し、これらと図4(C)に示す公開鍵証明書データ CER_{cp} とを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103に配給する

【0186】

ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、セキュアコンテナ104を対応する期間の配信用鍵データKD₁～KD₃などを用いて復号し、セキュアコンテナ104の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテナ104が正当なコンテンツプロバイダ101から送信されたか否かを確認する。

【0187】

ステップS5：SAM105₁～SAM105₄において、ユーザによる図9に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。

このとき、図15に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

【0188】

ステップS6：SAM105₁～SAM105₄の図15に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0189】

ステップS7：EMDサービスセンタ102は、図8に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG₉₉を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0190】

ステップS8： 決済機関91において、署名データSIG₉₉の検証を行った

後に、決済請求権データ 152 に基づいて、ユーザが支払った金額が、コンテンツプロバイダ 101 の所有者に分配される。

【0191】

第 1 実施形態の第 1 変形例

上述した実施形態では、図 4 (B) に示すように、コンテンツプロバイダ 101 において配信用鍵データ KD を用いてキーファイル KF を暗号化し、SAM105₁ ~ 105₄ において配信用鍵データ KD を用いてキーファイル KF を復号する場合を例示したが、図 1 に示すように、コンテンツプロバイダ 101 から SAM105₁ ~ 105₄ にセキュアコンテナ 104 を直接供給する場合には、配信用鍵データ KD を用いたキーファイル KF の暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データ KD を用いてキーファイル KF を暗号化することは、後述する第 2 実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データ KD をコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第 1 実施形態の場合でも、配信用鍵データ KD を用いてキーファイル KF を暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【0192】

また、上述した実施形態では、図 4 (B) に示すキーファイル KF 内の権利書データ 106 内に標準小売価格データ SRP を格納する場合を例示したが、セキュアコンテナ 104 内のキーファイル KF の外に、標準小売価格データ SRP (プライスタグデータ) を格納してもよい。この場合には、標準小売価格データ SRP に対して秘密鍵データ K_{cp} を用いて作成した署名データを添付する。

【0193】

第 1 実施形態の第 2 変形例

上述した第 1 実施形態では、図 1 に示すように、EMD サービスセンタ 102 が、自らが生成した決済請求権データ 152 を用いて、ペイメントゲートウェイ

90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図30に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

【0194】

第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄に、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a、101bからSAM105₁～105₄にそれぞれセキュアコンテナ104a、104bを供給するようにしてもよい。

図31は、コンテンツプロバイダ101a、101bを用いる場合の第1実施形態の第2変形例に係わるEMDシステムの構成図である。

この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれ6カ月分の配信用鍵データKD a₁～KD a₆およびKD b₁～KD b₆を配信する。

また、EMDサービスセンタ102は、SAM105₁～105₄に、3カ月分の配信用鍵データKD a₁～KD a₃およびKD b₁～KD b₃を配信する。

【0195】

そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データK c aを用いて暗号化したコンテンツファイルC F aと、コンテンツ鍵データK c aおよび権利書データ106aなどを対応する期間の配信用鍵データKD a₁～KD a₆を用いて暗号化したキーファイルK F aとを格納したセキュアコンテナ104aをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子Content __IDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKcbを用いて暗号化したコンテンツファイルCFbと、コンテンツ鍵データKcbおよび権利書データ106bなどを対応する期間の配信用鍵データKDb₁~KDb₆を用いて暗号化したキーファイルKFbとを格納したセキュアコンテナ104bをSAM105₁~105₄にオンラインおよび／またはオフランで供給する。
【0196】

SAM105₁~105₄は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKDa₁~KDa₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。

また、SAM105₁~105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKDb₁~KDb₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

【0197】

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

【0198】

また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKFa, KFbに対して、グローバルユニークな識別子Content_IDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 10

1 b の公開鍵証明書データ CER_{cpa} , CER_{CPb} を発行し、これに自らの署名データ $SIG_{1b,ESC}$, $SIG_{1a,ESC}$ を付してその正当性を認証する。

【0199】

第2実施形態

上述した実施形態では、コンテンツプロバイダ 101 からユーザホームネットワーク 103 の $SAM_{105_1} \sim 105_4$ にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークの SAM に配給する場合について説明する。

【0200】

図 32 は、本実施形態の EMD システム 300 の構成図である。

図 32 に示すように、EMD システム 300 は、コンテンツプロバイダ 301、EMD サービスセンタ 302、ユーザホームネットワーク 303、サービスプロバイダ 310、ペイメントゲートウェイ 90 および決済機関 91 を有する。

コンテンツプロバイダ 301、EMD サービスセンタ 302、 $SAM_{305_1} \sim 305_4$ などおよびサービスプロバイダ 310 は、それぞれ請求項 12 に係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ 301 は、サービスプロバイダ 310 に対してコンテンツデータを供給する点を除いて、前述した第 1 実施形態のコンテンツプロバイダ 101 と同じである。

また、EMD サービスセンタ 302 は、コンテンツプロバイダ 101 および $SAM_{505_1} \sim 505_4$ に加えて、サービスプロバイダ 310 に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第 1 実施形態の EMD サービスセンタ 102 と同じである。

また、ユーザホームネットワーク 303 は、ネットワーク機器 360_1 および AV 機器 $360_2 \sim 360_4$ を有している。ネットワーク機器 360_1 は SAM_{305_1} および CA モジュール 311 を内蔵しており、AV 機器 $360_2 \sim 360_4$ はそれぞれ $SAM_{305_2} \sim 305_4$ を内蔵している。

ここで、SAM305₁～305₄は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM105₁～105₄と同じである。

【0201】

まず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106は、EMDサービスセンタ302に登録されて権威化（認証）される。

【0202】

また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD₆を用いて、コンテンツ鍵データKcおよび権利書データ106を暗号化し、それらを格納したキーファイルKFを作成する。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納したセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ310に供給する。

【0203】

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104が正当なコンテンツプロバイダ301によって作成されたものであるか、並びに送り主の正当性を確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテン

ツプロバイダ 301 が希望するコンテンツに対しての価格 (SRP) に、自らのサービスの価格を加算した価格を示すプライスタグデータ (PT) 312 を作成する。

そして、サービスプロバイダ 310 は、セキュアコンテナ 104 から取り出したコンテンツファイル CF およびキーファイル KF と、プライスタグデータ 312 と、これらに対しての自らの秘密鍵データ $K_{SP,S}$ による署名データとを格納したセキュアコンテナ 304 を作成する。

このとき、キーファイル KF は、配信用鍵データ $KD_1 \sim KD_6$ によって暗号化されており、サービスプロバイダ 310 は当該配信用鍵データ $KD_1 \sim KD_6$ を保持していないため、サービスプロバイダ 310 はキーファイル KF の中身を見たり、書き換えたりすることはできない。

また、EMD サービスセンタ 302 は、プライスタグデータ 312 を登録して権威化する。

【0204】

サービスプロバイダ 310 は、オンラインおよび／またはオフラインでセキュアコンテナ 304 をユーザホームネットワーク 303 に配給する。

このとき、オフラインの場合には、セキュアコンテナ 304 は $SAM305_1 \sim 305_4$ にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ 310 と CA モジュール 311 との間で相互認証を行い、セキュアコンテナ 304 をサービスプロバイダ 310 においてセッション鍵データ K_{SES} を用いた暗号化して送信し、CA モジュール 311 において受信したセキュアコンテナ 304 をセッション鍵データ K_{SES} を用いて復号した後に、 $SAM305_1 \sim 305_4$ に転送する。

【0205】

次に、 $SAM305_1 \sim 305_4$ において、セキュアコンテナ 304 を、EMD サービスセンタ 302 から配給された対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号した後に、署名データの検証処理を行う。

$SAM305_1 \sim 305_4$ に供給されたセキュアコンテナ 304 は、ネットワーク機器 360₁ および AV 機器 360₂ \sim 360₄ において、ユーザの操作に

応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM305₁ ~ 305₄ は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log) データ308として記録する。

利用履歴データ(履歴データまたは管理装置用履歴データ)308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。

【0206】

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

【0207】

本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。

すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁ ~ 305₄ において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106およびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。

また、EMDサービスセンタ302は、例えば、配信用鍵データKD₁ ~ KD₆ などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM305₁～SAM305₄から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機能を有する。

【0208】

以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

〔コンテンツプロバイダ301〕

図33は、コンテンツプロバイダ301の機能ブロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

図33に示すように、コンテンツプロバイダ301は、コンテンツマスターサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、EMDサービスセンタ管理部125およびサービスプロバイダ管理部324を有する。

【0209】

図33において、図2と同一符号を付した構成要素は、前述した第1実施形態において図2および図3を参照しながら説明した同一符号の構成要素と同じである。

すなわち、コンテンツプロバイダ301は、図2に示すSAM管理部124の代わりにサービスプロバイダ管理部324を設けた構成をしている。

サービスプロバイダ管理部324は、セキュアコンテナ作成部118から入力したセキュアコンテナ104を、オフラインおよび／またはオンラインで、図32に示すサービスプロバイダ310に提供する。セキュアコンテナ104には、第1実施形態と同様に、図4（A），（B），（C）に示すコンテンツファイル

CF およびその署名データ $SIG_{6,CP}$ と、キーファイル KF およびその署名データ $SIG_{7,CP}$ と、公開鍵証明書データ CER_{CP} およびその署名データ SIG_{1,ES_C} とが格納されている。

【0210】

サービスプロバイダ管理部 324 は、セキュアコンテナ 104 をオンラインでサービスプロバイダ 310 に配信する場合には、暗号化・復号部 121 においてセッション鍵データ K_{SES} を用いてセキュアコンテナ 104 を暗号化した後に、ネットワークを介してサービスプロバイダ 310 に配信する。

【0211】

また、図 3 に示したコンテンツプロバイダ 101 内でのデータの流れは、サービスプロバイダ 310 にも同様に適用される。

【0212】

〔サービスプロバイダ 310〕

サービスプロバイダ 310 は、コンテンツプロバイダ 301 から提供を受けたセキュアコンテナ 104 内のコンテンツファイル CF およびキーファイル KF と、自らが生成したプライスタグデータ 312 とを格納したセキュアコンテナ 304 を、オンラインおよび／またはオフラインで、ユーザホームネットワーク 303 のネットワーク機器 360_1 および AV 機器 $360_2 \sim 360_4$ に配給する。

サービスプロバイダ 310 によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0213】

図 34 は、サービスプロバイダ 310 の機能ブロック図である。

なお、図 34 には、コンテンツプロバイダ 301 から供給を受けたセキュアコンテナ 104 に応じたセキュアコンテナ 304 をユーザホームネットワーク 30

3に供給する際のデータの流れが示されている。

図34に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

【0214】

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図34を参照しながら説明する。

コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図4に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図33に示す相互認証部120と図34に示す相互認証部352との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

【0215】

次に、署名処理部354において、記憶部351に記憶されているセキュアコンテナ104の図4(C)に示す署名データ $SIG_{1,ESC}$ を、記憶部351から読み出したEMDサービスセンタ302の公開鍵データ $K_{ESC,P}$ を用いて検証し、その正当性が認められた後に、図4(C)に示す公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP,P}$ を取り出す。

次に、署名処理部354は、当該取り出した公開鍵データ $K_{CP,P}$ を用いて、記憶部351に記憶されているセキュアコンテナ104の図4(A)，(B)に示す署名データ $SIG_{6,CP}$ 、 $SIG_{7,CP}$ の検証を行う。

【0216】

次に、セキュアコンテナ作成部355は、署名データSIG_{6,CP}、SIG_{7,CP}の正当性が確認されると、記憶部351からコンテンツファイルCFと、キーファイルKFと、サービスプロバイダ310の公開鍵証明書データCER_{SP}およびその署名データSIG_{61,ESC}を読み出す。

【0217】

また、プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、これをセキュアコンテナ作成部355に出力する。

【0218】

また、署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データK_{SP,P}を用いて、署名データSIG_{62,SP}、SIG_{63,SP}、SIG_{64,SP}を作成し、これをセキュアコンテナ作成部355に出力する。

【0219】

次に、セキュアコンテナ作成部355は、図35(A)～(D)に示すように、コンテンツファイルCFおよびその署名データSIG_{62,SP}と、キーファイルKFおよびその署名データSIG_{63,ESC}と、プライスタグデータ312およびその署名データSIG_{64,SP}と、公開鍵証明書データCER_{SP}およびその署名データSIG_{61,ESC}とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。そして、セキュアコンテナ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。

このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテ

ンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

【0220】

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MH EG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML (Hyper TextMarkup Language) プロトコルが用いられる。

このとき、コンテンツファイルCFおよびキーファイルKFは、コンテンツプロバイダ301によって一元的に管理され、セキュアコンテナ304を送信するプロトコルに依存しない。すなわち、コンテンツファイルCFおよびキーファイルKFは、MH EGおよびHTMLのプロトコルをトンネリングした形でセキュアコンテナ304内に格納される。

【0221】

次に、ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび／またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データK_{SES}を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360₁に配信する。

【0222】

なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。

そして、ユーザホームネットワーク管理部357は、セキュアコンテナ304

と共に、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を、衛星を介してユーザホームネットワーク 303 に送信する。

また、例えば、マスタ鍵データ K_M を、ICカードなどに記憶してオフラインでユーザホームネットワーク 303 に配給する。

【0223】

また、ユーザホームネットワーク管理部 357 は、ユーザホームネットワーク 303 から、当該サービスプロバイダ 310 が配給したコンテンツデータ C に関しての SP 用購入履歴データ 309 を受信すると、これを記憶部 351 に書き込む。

サービスプロバイダ 310 は、将来のサービス内容を決定する際に、SP 用購入履歴データ 309 を参照する。また、ユーザ嗜好フィルタ生成部 920 は、SP 用購入履歴データ 309 に基づいて、当該 SP 用購入履歴データ 309 を送信した $SAM305_1 \sim 305_4$ のユーザの嗜好を分析してユーザ嗜好フィルタデータ 900 を生成し、これをユーザホームネットワーク管理部 357 を介してユーザホームネットワーク 303 の CA モジュール 311 に送信する。

【0224】

図 36 には、サービスプロバイダ 310 内における EMD サービスセンタ 302 との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ 310 の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMD サービスセンタ 302 に登録処理を行い、グローバルユニークな識別子 SP_ID を得ている。識別子 SP_ID は、記憶部 351 に記憶される。

【0225】

先ず、サービスプロバイダ 310 が、EMD サービスセンタ 302 に、自らの秘密鍵データ $K_{SP,S}$ に対応する公開鍵データ $K_{SP,S}$ の正当性を証明する公開鍵証明書データ CER_{SP} を要求する場合の処理を図 36 を参照しながら説明する。

先ず、サービスプロバイダ 310 は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{SP,S}$ を生成し、当該秘密鍵データ $K_{SP,S}$ に対応する公開鍵データ

$K_{SP,P}$ を作成して記憶部 351 に記憶する。

EMDサービスセンタ管理部 358、サービスプロバイダ 310 の識別子 SP_ID および公開鍵データ $K_{SP,P}$ を記憶部 351 から読み出す。

そして、EMDサービスセンタ管理部 358 は、識別子 SP_ID および公開鍵データ $K_{SP,P}$ を、EMDサービスセンタ 302 に送信する。

そして、EMDサービスセンタ管理部 348 は、当該登録に応じて、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ を EMDサービスセンタ 302 から入力して記憶部 351 に書き込む。

【0226】

次に、サービスプロバイダ 310 が、EMDサービスセンタ 302 にプライスタグデータ 312 を登録して権威化する場合の処理を図 36 を参照して説明する。

【0227】

この場合には、署名処理部 354 において、プライスタグデータ作成部 356 が作成したプライスタグデータ 312 と記憶部 351 から読み出したグローバルユニークな識別子 $Content_ID$ とを格納したモジュール Mod_{103} のハッシュ値が求められ、秘密鍵データ $K_{SP,S}$ を用いて署名データ $SIG_{80,SP}$ が生成される。

また、記憶部 351 から公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ が読み出される。

そして、図 37 に示すプライスタグ登録要求用モジュール Mod_{102} を、相互認証部 352 と EMDサービスセンタ 302 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化・復号部 353 において暗号化した後に、EMDサービスセンタ管理部 358 から EMDサービスセンタ 302 に送信する。

なお、モジュール Mod_{103} に、サービスプロバイダ 310 のグローバルユニークな識別子 SP_ID を格納してもよい。

【0228】

また、EMDサービスセンタ管理部 358 は、EMDサービスセンタ 302 か

ら受信した決済レポートデータ 307s を記憶部 351 に書き込む。

【0229】

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信したマーケティング情報データ 904 を記憶部 351 に記憶する。

マーケティング情報データ 904 は、サービスプロバイダ 310 が今後配給するコンテンツデータ C を決定する際に参考にされる。

【0230】

〔EMD サービスセンタ 302〕

EMD サービスセンタ 302 は、前述したように、認証局 (CA: Certificate Authority)、鍵管理 (Key Management) 局および権利処理 (Rights Clearing) 局としての役割を果たす。

図 38 は、EMD サービスセンタ 302 の機能の構成図である。

図 38 に示すように、EMD サービスセンタ 302 は、鍵サーバ 141、鍵データベース 141a、決済処理部 442、署名処理部 443、決算機関管理部 144、証明書・権利書管理部 445、CER データベース 445a、コンテンツプロバイダ管理部 148、CP データベース 148a、SAM 管理部 149、SAM データベース 149a、相互認証部 150、暗号化・復号部 151、サービスプロバイダ管理部 390、SP データベース 390a、ユーザ嗜好フィルタ生成部 901 およびマーケティング情報データ生成部 902 を有する。

図 38 において、図 7 および図 8 と同じ符号を付した機能ブロックは、第 1 実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

以下、図 38 において、新たな符号を付した機能ブロックについて説明する。

なお、図 38 には、EMD サービスセンタ 302 内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ 310 との間で送受信されるデータに関連するデータの流れが示されている。

また、図 39 には、EMD サービスセンタ 302 内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ 301 との間で送受信されるデータに関連するデータの流れが示されている。

また、図 40 には、EMD サービスセンタ 302 内の機能ブロック相互間のデ

ータの流れのうち、図32に示すSAM305₁～305₄ および決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0231】

決算処理部442は、図40に示すように、SAM305₁～305₄ から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312に基づいて決済処理を行う。なお、この際に、決済処理部442は、サービスプロバイダ310によるダンプの有无などを監視する。

決済処理部442は、決済処理により、図40に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図38および図40に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

ここで、決済請求権データ152c、152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

【0232】

ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したラインセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図41に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ304に格納されたコンテンツデータCを提供したコンテンツプロバイダ301の識別子CP_ID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SP_ID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子Media_ID、セキュアコンテナ304を配給を受けたSAM305₁～305₄ の識別子SAM_

ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【0233】

証明書・権利書管理部445は、CERデータベース445aに登録されて権威化された公開鍵証明書データCER_{cp}、公開鍵証明書データCER_{sp}および公開鍵証明書データCER_{SAM1}～CER_{SAM2}などを読み出すと共に、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データK_c、並びにサービスプロバイダ310のプライスタグデータ312などをCERデータベース445aに登録して権威化する。

このとき、証明書・権利書管理部445は、権利書データ106、コンテンツ鍵データK_cおよびプライスタグデータ312などのハッシュ値をとり、秘密鍵データK_{ESC,S}を用いた署名データを付して権威化証明書データを作成する。

【0234】

コンテンツプロバイダ管理部148は、コンテンツプロバイダ101との間で通信する機能を有し、登録されているコンテンツプロバイダ101の識別子CP_IDなどを管理するCPデータベース148aにアクセスできる。

【0235】

ユーザ嗜好フィルタ生成部901は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM305₁～305₄のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM305₁～305₄に送信する。

【0236】

マーケティング情報データ生成部902は、利用履歴データ308に基づいて

、例えば、複数のサービスプロバイダ 310 によってユーザホームネットワーク 103 に配給されたコンテンツデータ C の全体の購入状況などを示すマーケティング情報データ 904 を生成し、これをサービスプロバイダ管理部 390 を介して、サービスプロバイダ 310 に送信する。サービスプロバイダ 310 は、マーケティング情報データ 904 を参考にして、今後提供するサービスの内容を決定する。

【0237】

以下、EMD サービスセンタ 302 内での処理の流れを説明する。

EMD サービスセンタ 302 からコンテンツプロバイダ 301 への配信用鍵データ $KD_1 \sim KD_6$ の送信と、EMD サービスセンタ 302 から $SAM_{305_1} \sim 305_4$ への配信用鍵データ $KD_1 \sim KD_3$ の送信とは、第 1 実施形態の場合と同様に行なわれる。

【0238】

また、EMD サービスセンタ 302 がコンテンツプロバイダ 301 から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部 445 が CER データベース 445a に対して登録を行なう点を除いて、前述した第 1 実施形態の場合と同様に行なわれる。

【0239】

次に、EMD サービスセンタ 302 がサービスプロバイダ 310 から、公開鍵証明書データの発行要求を受けた場合の処理を、図 38 を参照しながら説明する。

この場合に、サービスプロバイダ管理部 390 は、予め EMD サービスセンタ 302 によって与えられたサービスプロバイダ 310 の識別子 SP_ID 、公開鍵データ $K_{SP,P}$ および署名データ $SIG_{70,SP}$ をサービスプロバイダ 310 から受信すると、これらを、相互認証部 150 と図 34 に示す相互認証部 352 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_{70,SP}$ の正当性を署名処理部 443 において確認した後に、識別子 SP_ID および公開鍵データ $K_{SP,P}$ に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ 310 が SP デ

ータベース390aに登録されているか否かを確認する。

そして、証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データ CER_{SP} を CER データベース445aから読み出してサービスプロバイダ管理部390に出力する。

た、署名処理部443は、公開鍵証明書データ CER_{SP} のハッシュ値をとり、EMDサービスセンタ302の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{61,ESC}$ を作成し、これをサービスプロバイダ管理部390に出力する。

そして、サービスプロバイダ管理部390は、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ を、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0240】

なお、EMDサービスセンタ302が $SAM105_1 \sim 105_4$ から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106の登録要求を受けた場合の処理も、第1実施形態と同様である。

【0241】

次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図38を参照しながら説明する。

この場合には、サービスプロバイダ管理部390がサービスプロバイダ310から図37に示すプライスタグ登録要求モジュール Mod_{102} を受信すると、相互認証部150と図34に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いてプライスタグ登録要求モジュール Mod_{102} を復号する。

そして、当該復号したプライスタグ登録要求モジュール Mod_{102} に格納された署名データ $SIG_{80,SP}$ の正当性を署名処理部443において確認した後に、プライスタグ登録要求モジュール Mod_{102} に格納されたプライスタグデータ312を、証明書・権利書管理部445を介して CER データベース445aに登録

録して権威化する。

【0242】

次に、EMDサービスセンタ302において決済を行なう場合の処理を図40を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク303の例えばSAM305₁から利用履歴データ308およびその署名データSIG_{205,SAM1}を入力すると、利用履歴データ308および署名データSIG_{205,SAM1}を、相互認証部150とSAM305₁～305₄との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM305₁の公開鍵データK_{SAM1,p}を用いて署名データSIG_{205,SAM1}の検証を行なった後に、決算処理部442に出力する。

【0243】

そして、決済処理部442は、SAM305₁から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図40に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図38および図40に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

【0244】

次に、決算機関管理部144は、決済請求権データ152c, 152sと、それらについて秘密鍵データK_{ESC,S}を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図32に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプ

ロバイダ 301 に支払われ、決済請求権データ 152s に示される金額の金銭がサービスプロバイダ 310 に支払われる。

【0245】

次に、EMD サービスセンタ 302 がコンテンツプロバイダ 301 およびサービスプロバイダ 310 に決済レポートデータ 307c および 307s を送信する場合の処理を説明する。

決算処理部 442 において決済が行なわれると、決算処理部 442 からコンテンツプロバイダ管理部 148 に決済レポートデータ 307c が出力される。

コンテンツプロバイダ管理部 148 は、決算処理部 442 から決済レポートデータ 307c を入力すると、これを、相互認証部 150 と図 33 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 301 に送信する。

また、決算処理部 442 において決済が行なわれると、決算処理部 442 からサービスプロバイダ管理部 390 に決済レポートデータ 307s が出力される。

サービスプロバイダ管理部 390 は、決算処理部 442 から決済レポートデータ 307s を入力すると、これを、相互認証部 150 と図 34 に示す相互認証部 352 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ 310 に送信する。

【0246】

EMD サービスセンタ 302 は、その他に、第 1 実施形態の EMD サービスセンタ 102 と同様に、SAM 305₁ ~ 305₄ の出荷時の処理と、SAM 登録リストの登録処理とを行なう。

【0247】

〔ユーザホームネットワーク 303〕

ユーザホームネットワーク 303 は、図 32 に示すように、ネットワーク機器 360₁ および A/V 機器 360₂ ~ 360₄ を有している。

ネットワーク機器 360₁ は、CA モジュール 311 および SAM 305₁ を内蔵している。また、A/V 機器 360₂ ~ 360₄ は、それぞれ SAM 305₂ ~ 305₄ を内蔵している。

SAM305₁ ~ 305₄ の相互間は、例えば、1394 シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器360₂ ~ 360₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器360₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0248】

以下、ネットワーク機器360₁ について説明する。

図42は、ネットワーク機器360₁ の構成図である。

図42に示すように、ネットワーク機器360₁ は、通信モジュール162、CAモジュール311、復号モジュール905、SAM305₁、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

図42において、図8と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

【0249】

通信モジュール162は、サービスプロバイダ310との間の通信処理を行う。

具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテンツ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310に電話回線などを介してSP用購入履歴データ309を受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0250】

図43は、CAモジュール311および復号モジュール905の機能ブロック図である。

図43に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。

相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データ K_{SES} を生成し、これを暗号化・復号部908に出力する。

【0251】

記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

【0252】

暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力し、記憶部907から読み出したマスタ鍵データ K_M を用いてワーク鍵データ K_W を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データ K_W を用いてスクランブル鍵データ K_{SCR} を復号し、当該復号したスクランブル鍵データ K_{SCR} を復号部910に出力する。

また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データ K_{SES} を用いて復号して復号モジュール905のセキュアコンテンツ選択部911に出力する。

また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データ K_{SES} を用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

【0253】

SP用購入履歴データ生成部909は、図42に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータCの購入操作に応じた操作信号

S165、またはSAM305₁からの利用制御状態データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履歴データ309を生成し、これを暗号化・復号部908に出力する。

SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0254】

なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0255】

復号モジュール905は、復号部910およびセキュアコンテナ選択部911を有する。

復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテナ304、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力する。

そして、復号部910は、暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W をCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データ K_{SCR} を入力する。

そして、復号部910は、暗号化されたセキュアコンテナ304を、スクランブル鍵データ K_{SCR} を用いて復号した後に、セキュアコンテナ選択部911に出力する。

【0256】

なお、セキュアコンテナ304が、MPEG2 Transport Stream方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet内のECM(Entitlement Control Message)からスクランブル鍵データ K_{SCR} を取り出し、EMM(Entitlement Management Message)からワーク鍵データ K_W

を取り出す。

ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【0257】

セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM305₁に出力する。

【0258】

次に、SAM305₁について説明する。

なお、SAM305₁は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図10～図24を用いて前述した第1実施形態のSAM105₁と基本的に行なう機能および構造を有している。

また、SAM305₂～305₄は、SAM305₁と基本的に同じ機能を有している。

すなわち、SAM305₁～305₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0259】

以下、SAM305₁の機能について詳細に説明する。

図44は、SAM305₁の機能の構成図である。

なお、図44には、サービスプロバイダ310からセキュアコンテナ304を入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図44に示すように、SAM305₁は、相互認証部170、暗号化・復号部171、172、173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管

理部 190、記憶部 192、メディア SAM 管理部 197、スタックメモリ 200、サービスプロバイダ管理部 580、課金処理部 587、署名処理部 598 および外部メモリ管理部 811 を有する。

なお、図 44 に示す SAM305₁ の所定の機能は、SAM105₁ の場合と同様に、CPU において秘密プログラムを実行することによって実現される。

図 44 において、図 10 と同じ符号を付した機能ブロックは、第 1 実施形態で説明した同一符号の機能ブロックと同じである。

【0260】

また、図 42 に示す外部メモリ 201 には、第 1 実施形態で説明した処理および後述する処理を経て、利用履歴データ 308 および SAM 登録リストが記憶される。

また、スタックメモリ 200 には、図 45 に示すように、コンテンツ鍵データ K_c 、権利書データ (UCP) 106、記憶部 192 のロック鍵データ K_{LOC} 、コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} 、サービスプロバイダ 310 の公開鍵証明書データ CER_{SP} 、利用制御状態データ (UCS) 366、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ およびプライスタグデータ 312 などが記憶される。

【0261】

以下、SAM305₁ の機能ブロックのうち、図 44 において新たに符号を付した機能ブロックについて説明する。

署名処理部 589 は、記憶部 192 あるいはスタックメモリ 200 から読み出した EMD サービスセンタ 302 の公開鍵データ $K_{ESC,P}$ 、コンテンツプロバイダ 301 の公開鍵データ $K_{cp,p}$ およびサービスプロバイダ 310 の公開鍵データ $K_{SP,P}$ を用いて、セキュアコンテナ 304 内の署名データの検証を行なう。

【0262】

課金処理部 587 は、図 46 に示すように、図 42 に示す購入・利用形態決定操作部 165 からの操作信号 S165 と、スタックメモリ 200 から読み出されたプライスタグデータ 312 とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部 587 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御状態データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0263】

また、課金処理部 587 は、課金処理において、利用履歴データ 308 を生成し、これを外部メモリ管理部 811 を介して外部メモリ 201 に書き込む。

ここで、利用履歴データ 308 は、第 1 実施形態の利用履歴データ 108 と同様に、EMD サービスセンタ 302 において、セキュアコンテナ 304 に関連したライセンス料の支払いを決定する際に用いられる。

【0264】

また、課金処理部 587 は、操作信号 S165 に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ 166 を生成し、これを外部メモリ管理部 811 を介して外部メモリ 201 に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 166 には、コンテンツの ID、購入形態、買い切り価格、当該コンテンツの購入が行なわれた SAM の SAM_ID、購入を行なったユーザの USER_ID などが記述されている。

【0265】

なお、決定された購入形態が再生課金である場合には、例えば、SAM305₁ からサービスプロバイダ 310 に利用制御状態データ 166 をリアルタイムに送信し、サービスプロバイダ 310 が EMD サービスセンタ 302 に、利用履歴データ 108 を SAM105₁ に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0266】

また、SAM305₁では、EMDサービスセンタ管理部185がEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図42に示す復号モジュール905から入力したセキュアコンテナ304が、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM305₁において、当該SAM305₁のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0267】

以下、SAM305₁内での処理の流れを説明する。

EMDサービスセンタ302から受信した配信用鍵データKD₁～KD₃を記憶部192に格納する際のSAM305₁内での処理の流れは、前述したSAM105₁の場合と同様である。

【0268】

次に、セキュアコンテナ304をサービスプロバイダ310から入力し、セキュアコンテナ304内のキーファイルKFを復号する際のSAM305₁内での処理の流れを図44を参照しながら説明する。

相互認証部170と図34に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図35に示すセキュアコンテナ304を復号する。

【0269】

次に、署名処理部589は、図35(D)に示す署名データ $SIG_{61,ESC}$ の検証を行なった後に、図35(D)に示す公開鍵証明書データ CER_{SP} 内に格納されたサービスプロバイダ310の公開鍵データ $K_{SP,P}$ を用いて、署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ の正当性を確認する。

サービスプロバイダ管理部580は、署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ の正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

【0270】

誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ダウンロードメモリ管理部182は、相互認証部170と図42に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

【0271】

次に、ダウンロードメモリ管理部182は、相互認証部170と図42に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図35(B)に示すキーファイルKFを読み出してセキュアコンテナ復号部183に出力する。

【0272】

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFを復号し、図35(B)に示す署名・証明書モジュール Mod_1 に格納された署名データ $SIG_{1,ESC}$ 、 $SIG_{2,cp} \sim SIG_{4,cp}$ を署名処理部589に出力する。

署名処理部589は、図35(B)に示す署名データ $SIG_{1,ESC}$ の検証を行なった後に、公開鍵証明書データ CER_{cp} 内に格納された公開鍵データ $K_{CP,P}$ を用いて署名データ $SIG_{2,cp} \sim SIG_{4,cp}$ の検証を行なう。

【0273】

次に、セキュアコンテナ復号部183は、署名データ $SIG_{2,cp} \sim SIG_{4,cp}$

の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0274】

以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図46を参照しながら説明する。

ユーザによる図42に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部587に出力されると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図42に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図42に示す復号部221において復号された後に、復号部222に出力される。

【0275】

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図42に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ1

96がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される

【0276】

そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

そして、課金処理部187において、決定された購入形態に応じた利用履歴データ308および利用制御状態データ166が生成され、利用履歴データ308が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

そして、スタックメモリ200に格納されているキーファイルKFに、利用制御状態データ166が加えられ、購入形態が決定した後述する図47に示す新たなキーファイルKF₁₁が生成される。キーファイルKF₁₁は、スタックメモリ200に記憶される。

図47に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データK_{STR}を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をMAC鍵データとして用いて生成したMAC値であるMAC₃₀₀が付されている。また、利用制御状態データ166およびMAC₃₀₀からなるモジュールは、メディア鍵データMEDを用いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をMAC鍵データとして用いて生成したMAC値であるMAC₃₀₁が付されている。

【0277】

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図46を参照しながら説明する。

この場合には、利用監視部 186 の監視下で、操作信号 S165 に基づいて、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、図 42 に示す復号・伸長モジュール 163 に出力される。

また、スタックメモリ 200 から読み出されたコンテンツ鍵データ Kc が復号・伸長モジュール 163 に出力される。

そして、復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ Kc を用いたコンテンツファイル CF の復号と、伸長部 223 による伸長処理とが行なわれ、再生モジュール 169 において、コンテンツデータ C が再生される。

このとき、課金処理部 587 において、操作信号 S165 に応じて、利用履歴データ 308 が更新される。

利用履歴データ 308 は、秘密鍵データ $K_{SAM1,S}$ を用いて作成したそれぞれ署名データ $SIG_{205,SAM1}$ と共に、EMD サービスセンタ管理部 185 を介して、所定のタイミングで、EMD サービスセンタ 302 に送信される。

【0278】

次に、図 48 に示すように、例えば、ネットワーク機器 360₁ のダウンロードメモリ 167 にダウンロードされた既に購入形態が決定されたコンテンツファイル CF を、バス 191 を介して、AV 機器 360₂ の SAM305₂ に転送する場合の SAM305₁ 内での処理の流れを図 49 を参照しながら説明する。

ユーザは、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所定のコンテンツを AV 機器 360₂ に転送することを指示し、当該操作に応じた操作信号 S165 が、課金処理部 587 に出力される。

これにより、課金処理部 587 は、操作信号 S165 に基づいて、スタックメモリ 200 に記憶されている利用履歴データ 308 を更新する。

【0279】

また、ダウンロードメモリ管理部 182 は、ダウンロードメモリ 167 から読み出した図 50 (A) に示すコンテンツファイル CF を SAM 管理部 190 に出力する。

また、スタックメモリ 200 から読み出した図 50 (B) に示す既に購入形態

が決定されたキーファイル KF_{11} を、署名処理部 589 および SAM 管理部 190 に出力する。

署名処理部 589 は、キーファイル KF_{11} の署名データ $SIG_{80, SAM1}$ を作成し、これを SAM 管理部 190 に出力する。

また、SAM 管理部 190 は、記憶部 192 から、図 50 (C) に示す公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{22, ESC}$ を読み出す。

【0280】

また、相互認証部 170 は、 $SAM305_2$ との間で相互認証を行って得たセッション鍵データ K_{SES} を暗号化・復号部 171 に出力する。

SAM 管理部 190 は、図 50 (A), (B), (C) に示すデータを、暗号化・復号部 171 において、セッション鍵データ K_{SES} を用いて暗号化した後に、図 49 に示す AV 機器 360_2 の $SAM305_2$ に出力する。

【0281】

以下、図 48 に示すように、 $SAM305_1$ から入力したコンテンツファイル CF などを、RAM 型などの記録媒体 (メディア) に書き込む際の $SAM305_2$ 内での処理の流れを、図 51 を参照しながら説明する。

【0282】

この場合には、 $SAM305_2$ の SAM 管理部 190 は、図 51 に示すように、図 50 (A) に示すコンテンツファイル CF、図 50 (B) に示すキーファイル KF_{11} およびその署名データ $SIG_{80, SAM1}$ と、図 50 (C) に示す公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22, ESC}$ とを、ネットワーク機器 360_1 の $SAM305_1$ から入力する。

そして、暗号化・復号部 171 において、SAM 管理部 190 が入力したコンテンツファイル CF と、キーファイル KF_{11} およびその署名データ $SIG_{80, SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22, ESC}$ とが、相互認証部 170 と $SAM305_1$ の相互認証部 170 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて復号される。

【0283】

次に、セッション鍵データ K_{SES} を用いて復号されたコンテンツファイル CF

がメディアSAM管理部197に出力される。

また、セッション鍵データ K_{SES} を用いて復号されたキーファイル KF_{11} およびその署名データ $SIG_{80,SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、スタックメモリ200に書き込まれる。

【0284】

次に、署名処理部589は、スタックメモリ200から読み出した署名データ $SIG_{22,ESC}$ を、記憶部192から読み出した公開鍵データ $K_{ESC,P}$ を用いて検証して、公開鍵証明書データ CER_{SAM1} の正当性を確認する。

そして、署名処理部589は、公開鍵証明書データ CER_{SAM1} の正当性を確認すると、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1,P}$ を用いて、署名データ $SIG_{80,SAM1}$ の正当を確認する。

【0285】

次に、署名データ $SIG_{80,SAM1}$ の正当を確認されると、図50(B)に示すキーファイル KF_{11} をスタックメモリ200から読み出して暗号化・復号部173に出力する。

そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いてキーファイル KF_{11} を順に暗号化してメディアSAM管理部197に出力する。

【0286】

メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイル KF_{11} を、図48に示す記録モジュール260に出力する。

そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイル KF_{11} を、図48に示すRAM型の記録媒体250のRAM領域251に書き込む。

【0287】

なお、 $SAM305_1$ 内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器360₂内での処理の流れ、AV機器360₃において購入形態が未決定のROM型の記録媒体からセキュ

アコンテナ304を読み出してこれをAV機器360₂に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ312を格納する点を除いて、第1実施形態のSAM105₁の場合と同じである。

【0288】

次に、図32に示すEMDシステム300の全体動作について説明する。

図52および図53は、EMDシステム300の全体動作のフローチャートである。

ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテナ304を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄の登録は既に終了しているものとする。

【0289】

ステップS21：EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} を、自らの署名データ SIG_1, ESC と共にコンテンツプロバイダ301に送信する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ $K_{SP,P}$ の公開鍵証明書 CER_{SP} を、自らの署名データ $SIG_{61,ESC}$ と共にサービスプロバイダ310に送信する。

また、EMDサービスセンタ302は、各々有効期限が1カ月の6カ月分の配信用鍵データ $KD_1 \sim KD_6$ をコンテンツプロバイダ301に送信し、3カ月分の配信用鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク303のSAM305₁～305₄に送信する。

【0290】

ステップS22：コンテンツプロバイダ301は、図6(A)に示す権利登録要求モジュール Mod_2 を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利

書データ106およびコンテンツ鍵データKcを登録して権威化（認証）する。

【0291】

ステップS23：コンテンツプロバイダ301は、署名データの作成処理や、SIG対応する期間の配信用鍵データKD₁～KD₃などを用いた暗号化処理を経て、図4（A），（B），（C）に示すデータを格納したセキュアコンテナ104を、サービスプロバイダ310に供給する。

【0292】

ステップS24：サービスプロバイダ310は、図4（C）に示す署名データSIG_{1,ESC}を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、図4（A），（B）に示す署名データSIG_{6,CP}およびSIG_{7,CP}を検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0293】

ステップS25：サービスプロバイダ310は、プライスタグデータ312を作成し、プライスタグデータ312を格納した図35に示すセキュアコンテナ304を作成する。

【0294】

ステップS26：サービスプロバイダ310は、図37に示すプライスタグ登録要求モジュールMod₁₀₂を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

【0295】

ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図42に示すネットワーク機器360₁の復号モジュール905に送信する。

【0296】

ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0297】

ステップS29: SAM305₁ ~ 305₄ のいずれかにおいて、図35 (D) に示す署名データSIG_{61,ESC}を検証した後に、公開鍵証明書データCER_{SP}に格納された公開鍵データK_{SP,P}を用いて、図35 (A), (B), (C) に示す署名データSIG_{62,SP}、SIG_{63,SP}、SIG_{64,SP}を検証して、セキュアコンテナ304が正当なサービスプロバイダ310から送信されたものであるかを確認する。

【0298】

ステップS30: SAM305₁ ~ 305₄ のいずれかにおいて、配信用鍵データKD₁ ~ KD₃を用いて、図35 (B) に示すキーファイルKFを復号する。そして、SAM305₁ ~ 305₄ のいずれかにおいて、図35 (B) に示す署名データSIG_{1,ESC}を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、図35 (B) に示す署名データSIG_{2,CP}、SIG_{3,CP}およびSIG_{4,CP}を検証して、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106が正当なコンテンツプロバイダ301によって作成されたものであるかを確認する。

【0299】

ステップS31: ユーザが図42の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

【0300】

ステップS32: ステップS31において生成された操作信号S165に基づいて、SAM305₁ ~ 305₄ において、セキュアコンテナ304の利用履歴 (Usage Log) データ308が生成される。

SAM305₁ ~ 305₄ からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG_{205,SAM1}が送信される。

【0301】

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定 (計算) し、その結果に基づいて、決済請求権データ152c, 152s

を作成する。

【0302】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0303】

以上説明したように、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₄に供給される。従って、SAM305₁～305₄において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0304】

第2実施形態の第1変形例

図54は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。

図54において、図32と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

図54に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

【0305】

サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器360₁に配給する。

また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bとを格納したセキュアコンテナ304bを作成し、これをネットワーク機器360₁に配給する。

ここで、セキュアコンテナ304a、304bのフォーマットは、図35を用いた説明したセキュアコンテナ304と同じである。

【0306】

ネットワーク機器360a₁には、サービスプロバイダ310a、310bの各々に対応したCAモジュール311a、311bが設けられている。

CAモジュール311a、311bは、自らの要求に応じたセキュアコンテナ304a、304bの配給を、それぞれサービスプロバイダ310a、310bから受ける。

【0307】

次に、CAモジュール311a、311bは、配給されたセキュアコンテナ304a、304bに応じたSP用購入履歴データ309a、309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a、310bに送信する。

また、CAモジュール311a、311bは、セキュアコンテナ304a、304bをセッション鍵データK_{SES}で復号した後に、SAM305₁～305₄に出力する。

【0308】

次に、SAM305₁～305₄において、共通の配信用鍵データKD₁～KD₃を用いて、セキュアコンテナ304a、304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

【0309】

そして、SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0310】

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ152c、152sa、152sbを作成する。

【0311】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sa、152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a、310bの所有者に分配される。

【0312】

上述したように、EMDシステム300bによれば、同じコンテンツファイルCFをサービスプロバイダに310a、310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD₁～KD₆で暗号化してサービスプロバイダに310a、310bに供給し、サービスプロバイダに310a、310bは暗号化された権利書データ106をそのまま格納したセキュアコンテナ304a、304bをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のSAM305₁～305₄では、コンテンツファイルCFをサービスプロバイダに310a、310bの何れか

ら配給を受けた場合でも、共通の権利書データ 106 に基づいて権利処理を行うことができる。

【0313】

なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【0314】

第2実施形態の第2変形例

図55は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステム300bの構成図である。

図55において、図32と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

図55に示すように、EMDシステム300bでは、コンテンツプロバイダ301a、301bからサービスプロバイダ310に、それぞれセキュアコンテナ104a、104bが供給される。

【0315】

サービスプロバイダ310は、例えば、コンテンツプロバイダ301a、301bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104aについてのプライスタグデータ312aと、セキュアコンテナ104bについてのプライスタグデータ312bとをそれぞれ生成し、これらを格納したセキュアコンテナ304cを作成する。

図55に示すように、セキュアコンテナ304cには、コンテンツファイルCFa、CFb、キーファイルKFa、KFb、プライスタグデータ312a、312b、それらの各々についてのサービスプロバイダ310の秘密鍵データ $K_{CP,S}$ による署名データが格納されている。

【0316】

セキュアコンテナ304cは、ユーザホームネットワーク303のネットワーク機器360₁のCAモジュール311で受信された後に、SAM305₁～305₄において処理される。

【0317】

SAM305₁ ~ 305₄ では、配信用鍵データ KDa₁ ~ KDa₃ を用いて、キーファイル KFa が復号され、権利書データ 106a に基づいて、コンテンツファイル CFa についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

また、SAM305₁ ~ 305₄ において、配信用鍵データ KDb₁ ~ KDb₃ を用いて、キーファイル KFb が復号され、権利書データ 106b に基づいて、コンテンツファイル CFb についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

【0318】

そして、SAM305₁ ~ 305₄ から EMD サービスセンタ 302 に、利用履歴データ 308 が送信される。

【0319】

EMD サービスセンタ 302 では、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301a, 301b およびサービスプロバイダ 310 の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152ca, 152cb, 152s を作成する。

【0320】

EMD サービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152ca, 152cb, 152s を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301a, 301b およびサービスプロバイダ 310 の所有者に分配される。

【0321】

上述したように、EMD システム 300b によれば、セキュアコンテナ 304c 内に格納されたコンテンツファイル CFa, CFb の権利書データ 106a, 106b は、コンテンツプロバイダ 301a, 301b が作成したものをそのまま用いるため、SAM305₁ ~ 305₄ 内において、権利書データ 106a, 106b に基づいて、コンテンツファイル CFa, CFb についての権利処理が

コンテンツプロバイダ 301 a, 301 b の意向に沿って確実に行われる。

【0322】

なお、図 55 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【0323】

第 2 実施形態の第 3 変形例

図 56 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、EMD サービスセンタ 302 が決済機関 91 に対して、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済を行う場合を例示したが、本発明では、例えば、図 56 に示すように、EMD サービスセンタ 302 において、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 のための決済請求権データ 152 c と、サービスプロバイダ 310 のための決済請求権データ 152 s とを作成し、これらをそれぞれコンテンツプロバイダ 301 およびサービスプロバイダ 310 に送信するようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、決済請求権データ 152 c を用いて、ペイメントゲートウェイ 90 a を介して決済機関 91 a に決済を行う。また、サービスプロバイダ 310 は、決済請求権データ 152 s を用いて、ペイメントゲートウェイ 90 b を介して決済機関 91 b に決済を行う。

【0324】

第 2 実施形態の第 4 変形例

図 57 は、第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、例えば現行のインターネットのようにサービスプロバイダ 310 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 310 が課金機能を有している場合には、CA モジュール 311 において、セキュアコンテナ 304 に関するサービスプロバ

イダ310のサービスに対しての利用履歴データ308sを作成してサービスプロバイダ310に送信する。

そして、サービスプロバイダ310は、利用履歴データ308sに基づいて、課金処理を行って決済請求権データ152sを作成し、これを用いてペイメントゲートウェイ90bを介して決済機関91bに決済を行う。

一方、SAM305₁～305₄は、セキュアコンテナ304に関するコンテンツプロバイダ301の権利処理に対しての利用履歴データ308cを作成し、これをEMDサービスセンタ302に送信する。

EMDサービスセンタ302は、利用履歴データ308cに基づいて、決済請求権データ152cを作成し、これをコンテンツプロバイダ301に送信する。

コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。

【0325】

第2実施形態の第5変形例

上述した実施形態では、図40に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM305₁などから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図46に示すSAM305₁などの利用監視部186で生成した利用制御状態データ166をリアルタイムでEMDサービスセンタ302に送信するようにして、SP用購入履歴データ309において、利用制御状態データ166に基づいてユーザ嗜好フィルタデータ903を生成するようにしてもよい。

【0326】

第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄は、それぞれ自らの公開鍵データ $K_{CP,P}$ 、 $K_{SP,P}$ 、 $K_{SAM1,P}$ ～ $K_{SAM4,P}$ の他に、自らの秘密鍵データ $K_{CP,S}$ 、 $K_{SP,S}$ 、 $K_{SAM1,S}$ ～ $K_{SAM4,S}$ をEMDサービスセンタ302に登録してもよい。

このようにすることで、EMDサービスセンタ302は、緊急時に、国家ある

いは警察機関などからの要請に応じて、秘密鍵データ $K_{CP,S}$, $K_{SP,S}$, $K_{SAM1,S}$ ~ $K_{SAM4,S}$ を用いて、コンテンツプロバイダ 301 とサービスプロバイダ 310 との間の通信、サービスプロバイダ 310 と $SAM305_1$ ~ 305_4 との間の通信、並びにユーザホームネットワーク 303 内での $SAM305_1$ ~ 305_4 相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、 $SAM305_1$ ~ 305_4 については、出荷時に、EMD サービスセンタ 302 によって秘密鍵データ $K_{SAM1,S}$ ~ $K_{SAM4,S}$ を生成し、これを $SAM305_1$ ~ 305_4 に格納すると共に EMD サービスセンタ 302 が保持（登録）するようにしてもよい。

【0327】

第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1$ ~ 305_4 が、相互に通信を行う場合に、EMD サービスセンタ 302 から事前に公開鍵証明書データ CER_{CP} , CER_{SP} , CER_{SAM1} ~ CER_{SAM4} を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1$ ~ 305_4 が、相互に通信を行う場合に、EMD サービスセンタ 302 から事前に公開鍵証明書データ CER_{CP} , CER_{SP} , CER_{SAM1} ~ CER_{SAM4} を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1$ ~ 305_4 が、通信時に、EMD サービスセンタ 302 から公開鍵証明書データ CER_{CP} , CER_{SP} , CER_{SAM1} ~ CER_{SAM4} を取得してもよい。

【0328】

図 58 は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。

なお、図 58 において、図 32 と同じ符号を付した構成要素は、前述した同一

符号の構成要素と同じである。また、ユーザホームネットワーク 303a は、前述したユーザホームネットワーク 303 と同じである。ユーザホームネットワーク 303b では、IEEE 1394 シリアルバスであるバス 191 を介して SAM305₁₁ ~ 305₁₄ を接続している。

【0329】

コンテンツプロバイダ 301 がサービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ 310 からコンテンツプロバイダ 301 に公開鍵証明書データ CER_{SP} を送信する場合（図 58 中（3））と、コンテンツプロバイダ 301 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SP} を取り寄せる場合（図 58 中（1））とがある。

【0330】

また、サービスプロバイダ 310 がコンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ 301 からサービスプロバイダ 310 に公開鍵証明書データ CER_{CP} を送信する場合（図 58 中（2））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{CP} を取り寄せる場合（図 58 中（4））とがある。

【0331】

また、サービスプロバイダ 310 が SAM305₁ ~ 305₄ の公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を取得する場合には、例えば、通信に先立って SAM305₁ ~ 305₄ からサービスプロバイダ 310 に公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を送信する場合（図 58 中（6））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を取り寄せる場合（図 58 中（4））とがある。

【0332】

また、SAM305₁ ~ 305₄ がサービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ 310 から SAM305₁ ~ 305₄ に公開鍵証明書データ CER_{SP} を送信す

る場合（図58中（5））と、 $SAM305_1 \sim 305_4$ がEMDサービスセンタ302から公開鍵証明書データ CER_{SP} を取り寄せる場合（図58中（7）など）とがある。

【0333】

また、 $SAM305_1$ が $SAM305_2$ の公開鍵証明書データ CER_{SAM2} を取得する場合には、例えば、通信に先立って $SAM305_2$ から $SAM305_1$ に公開鍵証明書データ CER_{SAM2} を送信する場合（図58中（8））と、 $SAM305_1$ がEMDサービスセンタ302から公開鍵証明書データ CER_{SAM2} を取り寄せる場合（図58中（7）など）とがある。

【0334】

また、 $SAM305_2$ が $SAM305_1$ の公開鍵証明書データ CER_{SAM1} を取得する場合には、例えば、通信に先立って $SAM305_1$ から $SAM305_2$ に公開鍵証明書データ CER_{SAM1} を送信する場合（図58中（9））と、 $SAM305_2$ が自らEMDサービスセンタ302から公開鍵証明書データ CER_{SAM1} を取り寄せる場合と、 $SAM305_1$ が搭載されたネットワーク機器を介して公開鍵証明書データ CER_{SAM1} を取り寄せる場合（図58中（7），（8））とがある。

【0335】

また、 $SAM305_4$ が $SAM305_{13}$ の公開鍵証明書データ CER_{SAM13} を取得する場合には、例えば、通信に先立って $SAM305_{13}$ から $SAM305_4$ に公開鍵証明書データ CER_{SAM13} を送信する場合（図58中（12））と、 $SAM305_4$ が自らEMDサービスセンタ302から公開鍵証明書データ CER_{SAM13} を取り寄せる場合（図58中（10））と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データ CER_{SAM13} を取り寄せる場合とがある。

【0336】

また、 $SAM305_{13}$ が $SAM305_4$ の公開鍵証明書データ CER_{SAM4} を取得する場合には、例えば、通信に先立って $SAM305_4$ から $SAM305_{13}$ に公開鍵証明書データ CER_{SAM4} を送信する場合（図58中（11））と、 SAM

305₁₃が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM4}を取り寄せる場合(図58中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SAM4}を取り寄せる場合とがある。

【0337】

第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁~305₄が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁~305₄に送信する。

なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁~305₄において生成してもよい。

【0338】

先ず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}を無効にする場合について説明する。

図59に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{CP}を無効にすることを示す公開鍵証明書破棄データCRL₁をサービスプロバイダ310に送信する(図59中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{CP,P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【0339】

また、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_1 を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に送信する（図59中（1），（2））。 $SAM305_1$ は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データ CRL_1 を参照して公開鍵証明書データ CER_{CP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{CP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_1 を、ユーザホームネットワーク303内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい（図59中（3））。

【0340】

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データ CER_{SP} を無効にする場合について説明する。

図60に示すように、EMDサービスセンタ302は、公開鍵証明書データ CER_{SP} を無効にすることを示す公開鍵証明書破棄データ CRL_2 をコンテンツプロバイダ301に送信する（図60中（1））。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

【0341】

また、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_2 を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に送信する（図60中（2））。 $SAM305_1$ は、サービスプロバイダ310

から入力したセキュアコンテナ内に格納されたサービスプロバイダ 310 の署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ 310 内において、公開鍵証明書破棄データ CRL_2 の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ 310 内において、公開鍵証明書破棄データ CRL_2 は、サービスプロバイダ 310 の関係者による改竄な困難な領域に格納される必要がある。

なお、EMD サービスセンタ 302 は、公開鍵証明書破棄データ CRL_2 を、ユーザホームネットワーク 303 内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい（図 60 中（3））。

【0342】

次に、EMD サービスセンタ 302 が、例えば $SAM305_2$ の公開鍵証明書データ CER_{SAM2} を無効にする場合について説明する。

図 61 に示すように、EMD サービスセンタ 302 は、公開鍵証明書データ CER_{SAM2} を無効にすることを示す公開鍵証明書破棄データ CRL_3 をコンテンツプロバイダ 301 に送信する（図 61 中（1））。コンテンツプロバイダ 301 は、公開鍵証明書破棄データ CRL_3 をサービスプロバイダ 310 に送信する。サービスプロバイダ 310 は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク 303 内の例えば $SAM305_1$ に公開鍵証明書破棄データ CRL_{SAM1} を送信する（図 61 中（1））。 $SAM305_1$ は、 $SAM305_2$ から入力したデータに付加された $SAM305_2$ の署名データを検証する際に、公開鍵証明書破棄データ CRL_3 を参照して公開鍵証明書データ CER_{SAM2} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SAM2,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ 310 内において、公開鍵証明書破棄データ

CRL₃ の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

【0343】

EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい(図61中(1)、(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図61中(3))。

【0344】

また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃を作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図62中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図62中(1))。

SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0345】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをコンテンツプロバイダ301に送信する(図62中(2))。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する(図62中(2))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する(図62中(2))。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0346】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する(図62中(3))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する(図62中(3))。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0347】

EMDサービスセンタ302の役割等

図63は、図32に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

【0348】

また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。

また、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKcの登録（権威化）などを行う。

なお、図64に示すように、権利管理用クリアリングハウス950と電子決済用クリアリングハウス951とを単体の装置内に収納すると、図32に示すEMDサービスセンタ302となる。

【0349】

また、本発明は、例えば、図65に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス960の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス960からの決済請求権データに基づいて決済を行う。

【0350】

また、本発明は、例えば、図66に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス970の機能を設け、権利管理用クリアリングハウス970において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてコンテンツプロバイダ301の決済請求権データを作成し、これをコンテンツプロバイダ301に送信してもよい。この場合には、コンテンツプロバイダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970からの決済請求権データに基づいて決済を行う。

【0351】

【発明の効果】

以上説明したように、本発明のデータ提供システムおよびその方法と管理装置によれば、データ提供装置の関係者の利益が適切に保護される。

また、本発明のデータ提供システムおよびその方法と管理装置によれば、管理装置において権利書データなどの証明を行うため、例えば、権利書データなどが不正に改竄された場合などに適切に対処できる。

また、本発明のデータ提供システムおよびその方法と管理装置によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

【図面の簡単な説明】

【図1】

図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】

図2は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図である。

【図3】

図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 4】

図 4 は、図 1 に示すコンテンツプロバイダから SAM に送信されるセキュアコンテンツのフォーマットを説明するための図である。

【図 5】

図 5 は、ROM 型の記録媒体を説明するための図である。

【図 6】

図 6 (A) はコンテンツプロバイダから EMD サービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図 6 (B) は EMD サービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

【図 7】

図 7 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 8】

図 8 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、SAM および図 1 に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図 9】

図 9 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図 10】

図 10 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図である。

【図 11】

図 11 は、図 9 に示す外部メモリに記憶されるデータを説明するための図である。

【図 12】

図 12 は、スタックメモリに記憶されるデータを説明するための図である。

【図 13】

図 13 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図 14】

図 14 は、図 10 に示す記憶部に記憶されるデータを説明するための図である。

【図 15】

図 15 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図 16】

図 16 は、図 9 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送元の SAM 内での処理の流れを説明するための図である。

【図 17】

図 17 は、図 16 に示す場合における転送元の SAM 内でのデータの流れを示す図である。

【図 18】

図 18 は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図 19】

図 19 は、図 16 に示す場合において、転送先の SAM において、入力したコンテンツファイルなどを、RAM 型あるいは ROM 型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図 20】

図 20、コンテンツの購入形態が未決定の図 5 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において

購入形態を決定する際の処理の流れを説明するための図である。

【図 2 1】

図 2 1 は、図 2 0 に示す場合において、S A M 内でのデータの流れを示す図である。

【図 2 2】

図 2 2 は、ユーザホームネットワーク内の A V 機器において購入形態が未決定の R O M 型の記録媒体からセキュアコンテナを読み出して、これを他の A V 機器に転送して R A M 型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 2 3】

図 2 3 は、図 2 2 に示す場合における転送元の S A M 内でのデータの流れを示す図である。

【図 2 4】

図 2 4 は、図 2 2 に示す場合における転送先の S A M 内でのデータの流れを示す図である。

【図 2 5】

図 2 5 は、図 1 に示すコンテンツプロバイダ、E M D サービスセンタおよび S A M の相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 2 6】

図 2 6 は、図 1 に示すコンテンツプロバイダ、E M D サービスセンタおよび S A M の相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 2 7】

図 2 7 は、バス 1 9 1 への機器の接続形態の一例を説明するための図である。

【図 2 8】

図 2 8 は、S A M 登録リストのデータフォーマットを説明するための図である。

【図 29】

図 29 は、図 1 に示すコンテンツプロバイダの全体動作のフローチャートである。

【図 30】

本発明の第 1 実施形態の第 2 変形例を説明するための図である。

【図 31】

本発明の第 1 実施形態の第 3 変形例を説明するための図である。

【図 32】

図 30 は、本発明の第 2 実施形態の EMD システムの全体構成図である。

【図 33】

図 33 は、図 32 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図 34】

図 34 は、図 32 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図 35】

図 35 は、図 32 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図 36】

図 36 は、図 32 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図である。

【図 37】

図 37 は、サービスプロバイダから EMD サービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図 38】

図 38 は、図 32 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 3 9】

図 3 9 は、図 3 2 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 4 0】

図 4 0 は、図 3 2 に示す EMD サービスセンタの機能ブロック図であり、SAM との間で送受信されるデータに関連するデータの流れを示す図である。

【図 4 1】

図 4 1 は、利用履歴データの内容を説明するための図である。

【図 4 2】

図 4 2 は、図 3 2 に示すネットワーク機器の構成図である。

【図 4 3】

図 4 3 は、図 4 2 に示す CA モジュールの機能ブロック図である。

【図 4 4】

図 4 4 は、図 4 2 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図 4 5】

図 4 5 は、図 4 4 に示す記憶部に記憶されるデータを説明するための図である。

【図 4 6】

図 4 6 は、図 4 2 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図 4 7】

図 4 7 は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図 4 8】

図 4 8 は、図 4 2 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送先の SAM 内での処理の流れを説明するための図である。

【図 4 9】

図 4 9 は、図 4 8 に示す場合の転送元の SAM 内でのデータの流れを示す図である。

【図 5 0】

図 5 0 は、ネットワーク機器の SAM から AV 機器の SAM に転送される購入形態が既に決定されたセキュアコンテンツのフォーマットを説明するための図である。

【図 5 1】

図 5 1 は、図 4 8 に示す場合の転送先の SAM 内でのデータの流れを示す図である。

【図 5 2】

図 5 2 は、図 3 2 に示す EMD システムの全体動作のフローチャートである。

【図 5 3】

図 5 3 は、図 3 2 に示す EMD システムの全体動作のフローチャートである。

【図 5 4】

図 5 4 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システムの構成図である。

【図 5 5】

図 5 5 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システムの構成図である。

【図 5 6】

図 5 6 は、本発明の第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

【図 5 7】

図 5 7 は、本発明の第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

【図 5 8】

図 5 8 は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図 59】

図 59 は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 60】

図 60 は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 61】

図 61 は、SAM の公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 62】

図 62 は、SAM の公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図 63】

図 63 は、図 32 に示す EMD システムにおいて、EMD サービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図 64】

図 64 は、図 63 に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体の EMD サービスセンタ内に設けた場合の EMD システムの構成図である。

【図 65】

図 65 は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 66】

図 66 は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 67】

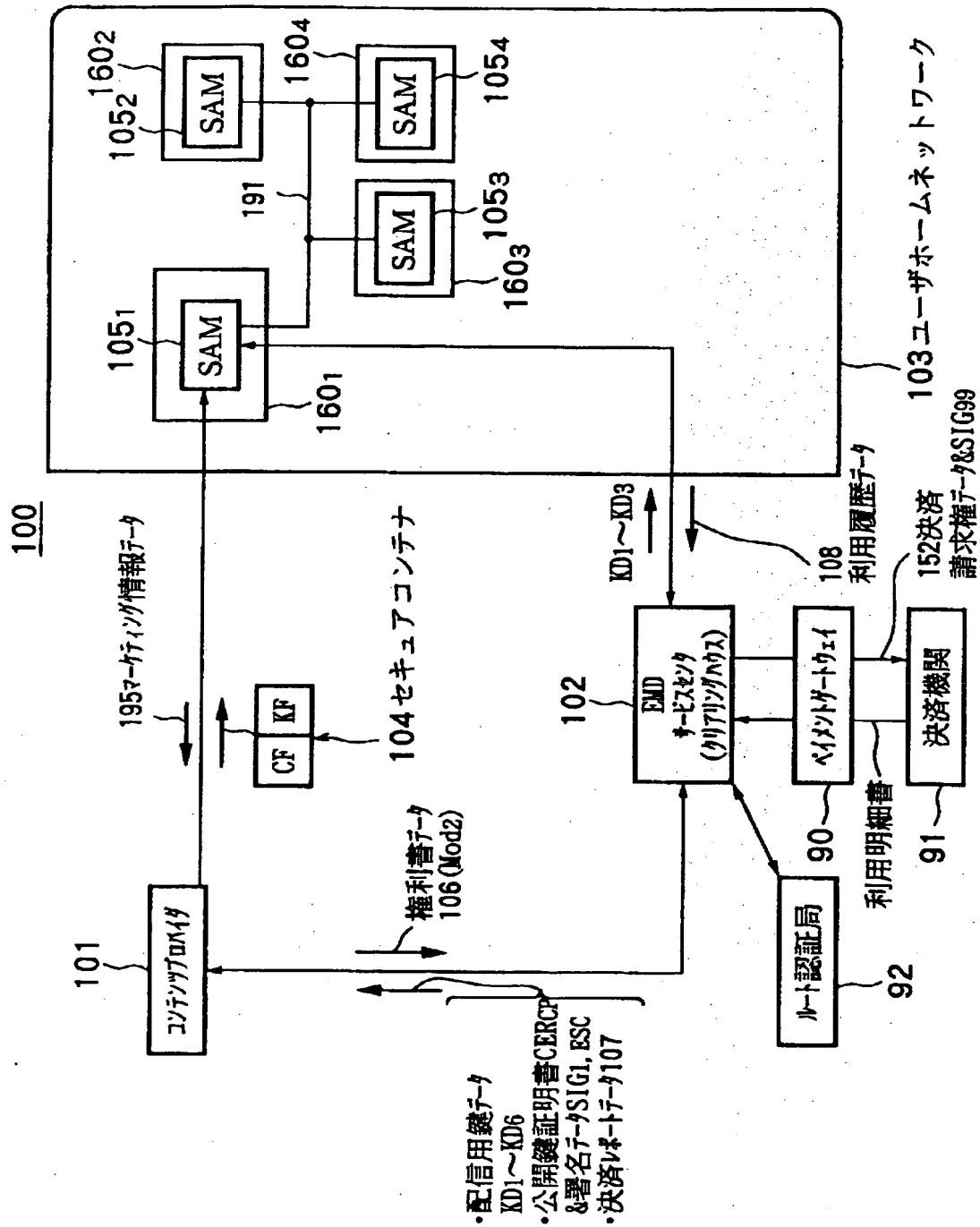
従来の EMD システムの構成図である。

【符号の説明】

90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100, 300…EMDシステム、101, 301…コンテンツプロバイダ、102, 302…EMDサービスセンタ、103, 303…ユーザホームネットワーク、104, 304…セキュアコンテナ、105₁～105₄, 305₁～305₄…SAM、106…権利書データ、107, 307…決済レポートデータ、108, 308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV機器、152, 152c, 152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

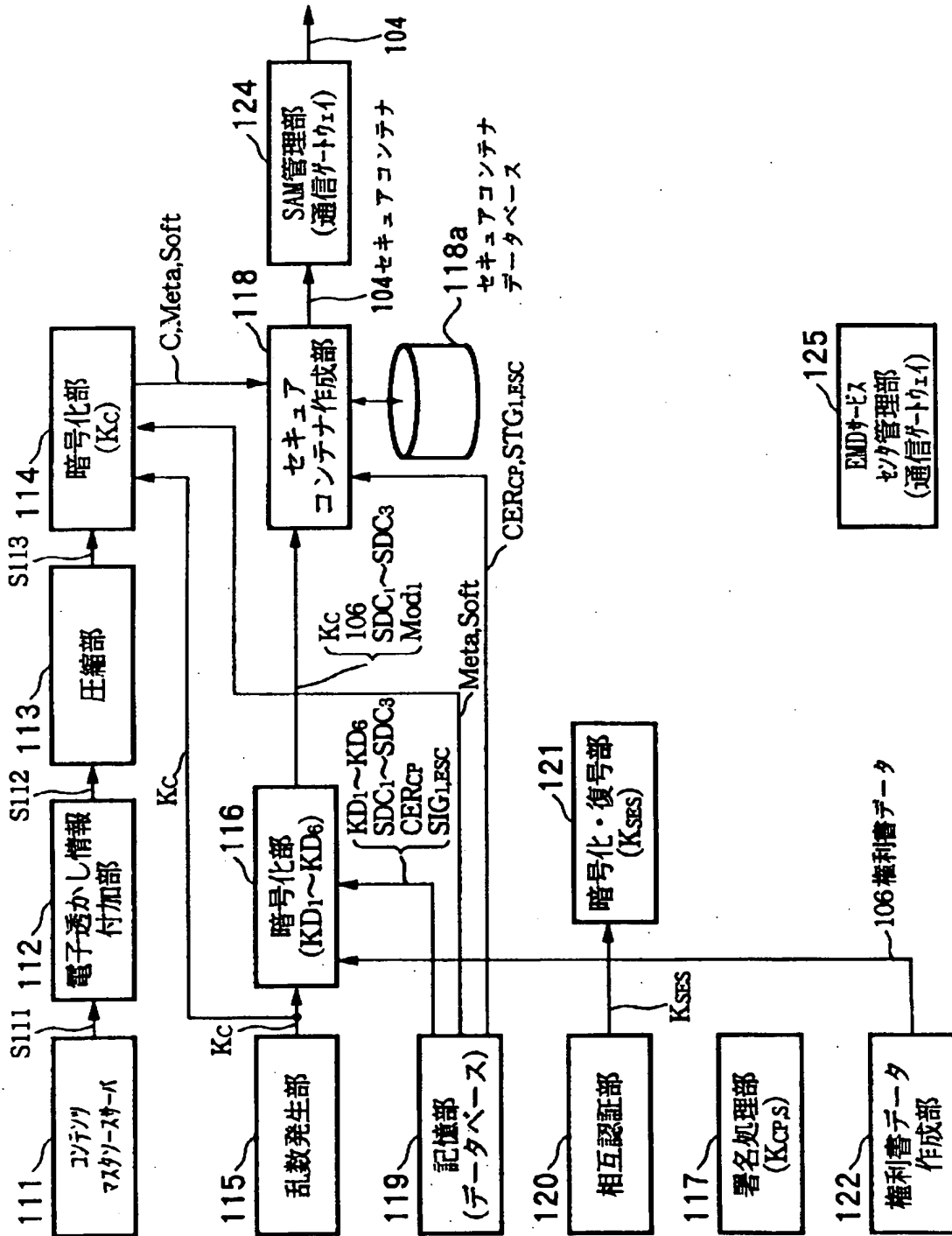
【書類名】 図面

【図 1】

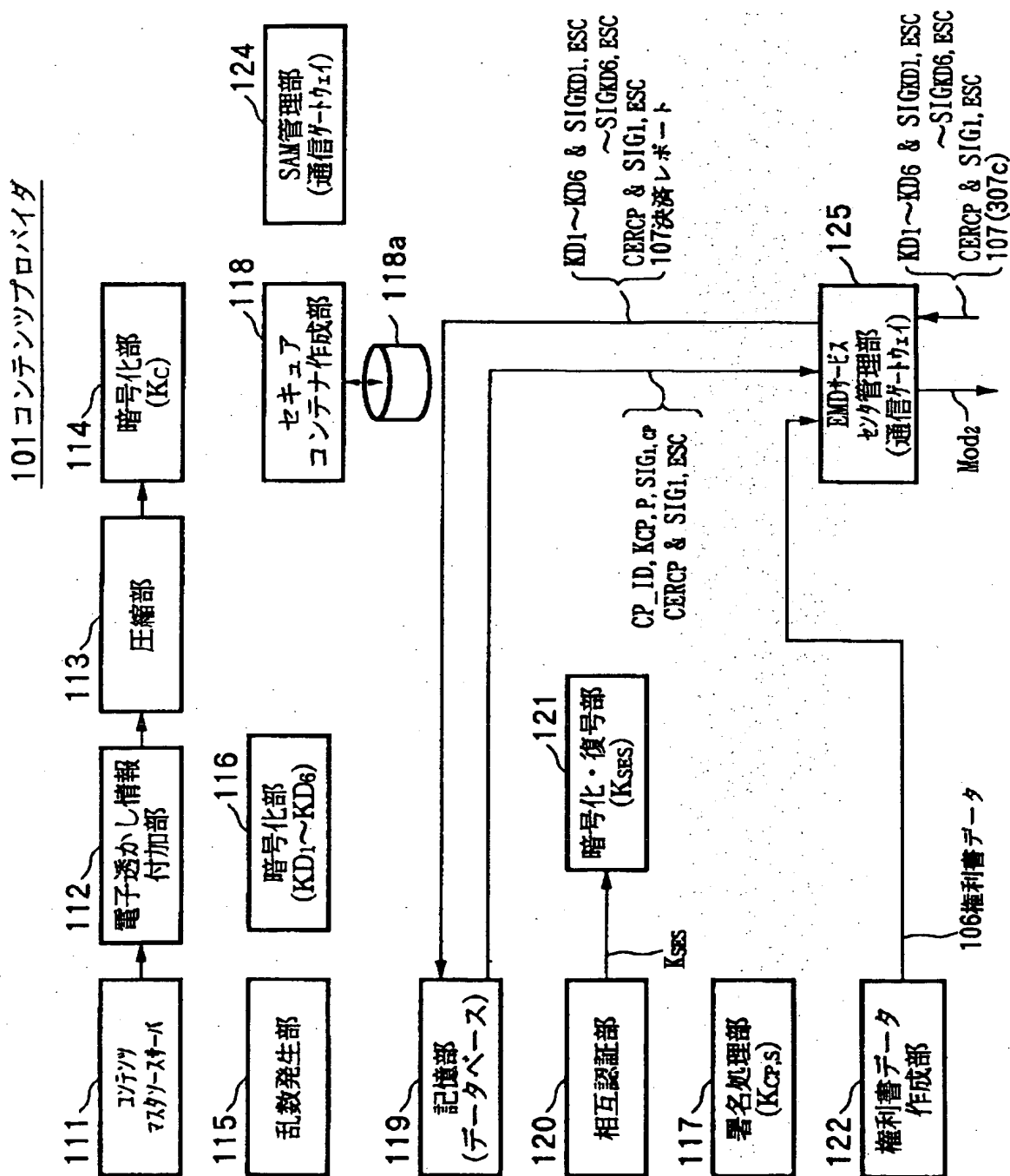


【図 2】

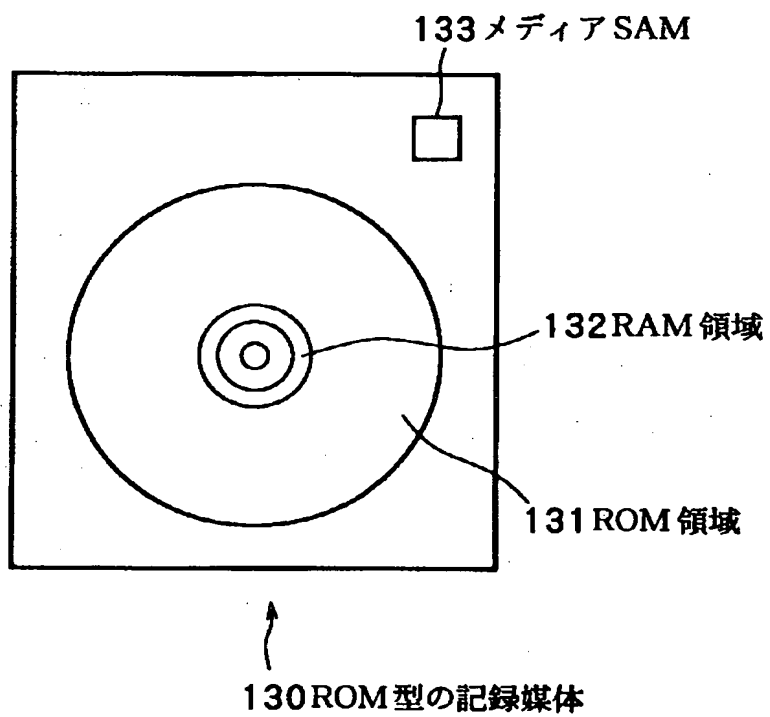
101 コンテンツプロバイダ



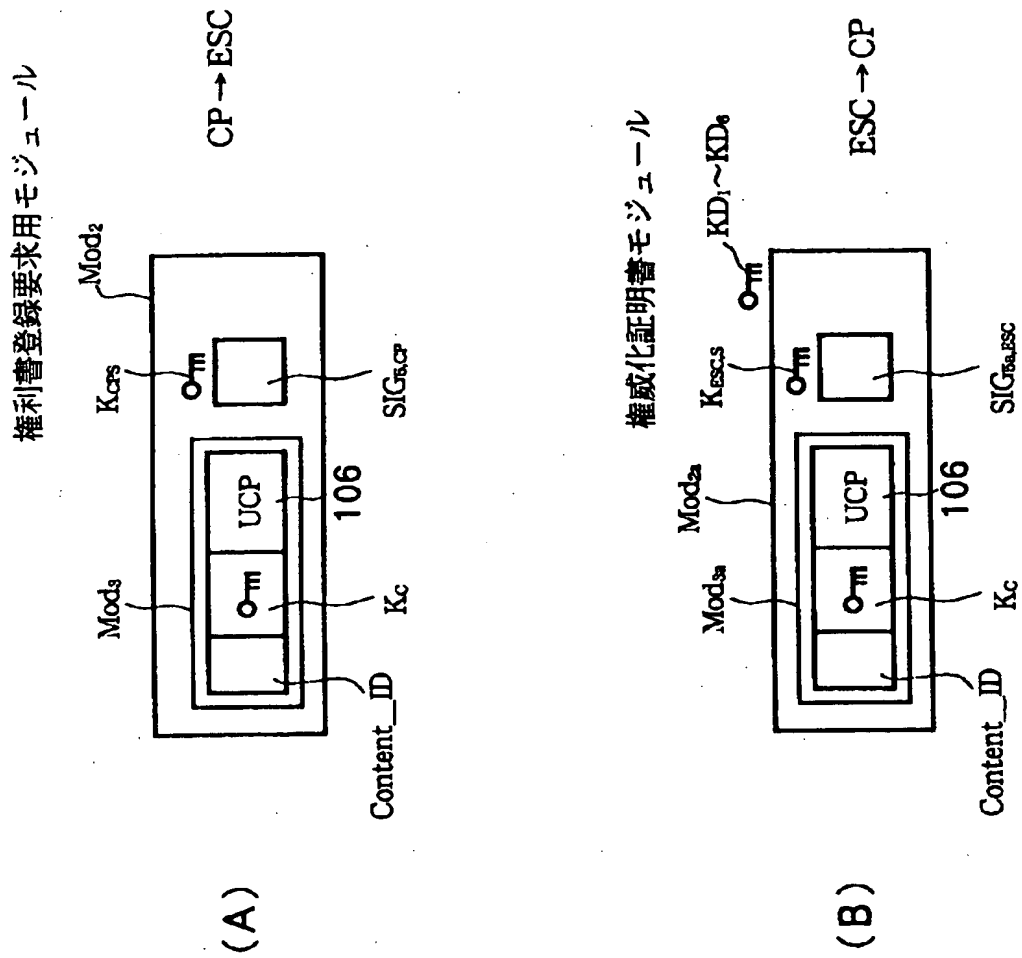
【图 3】



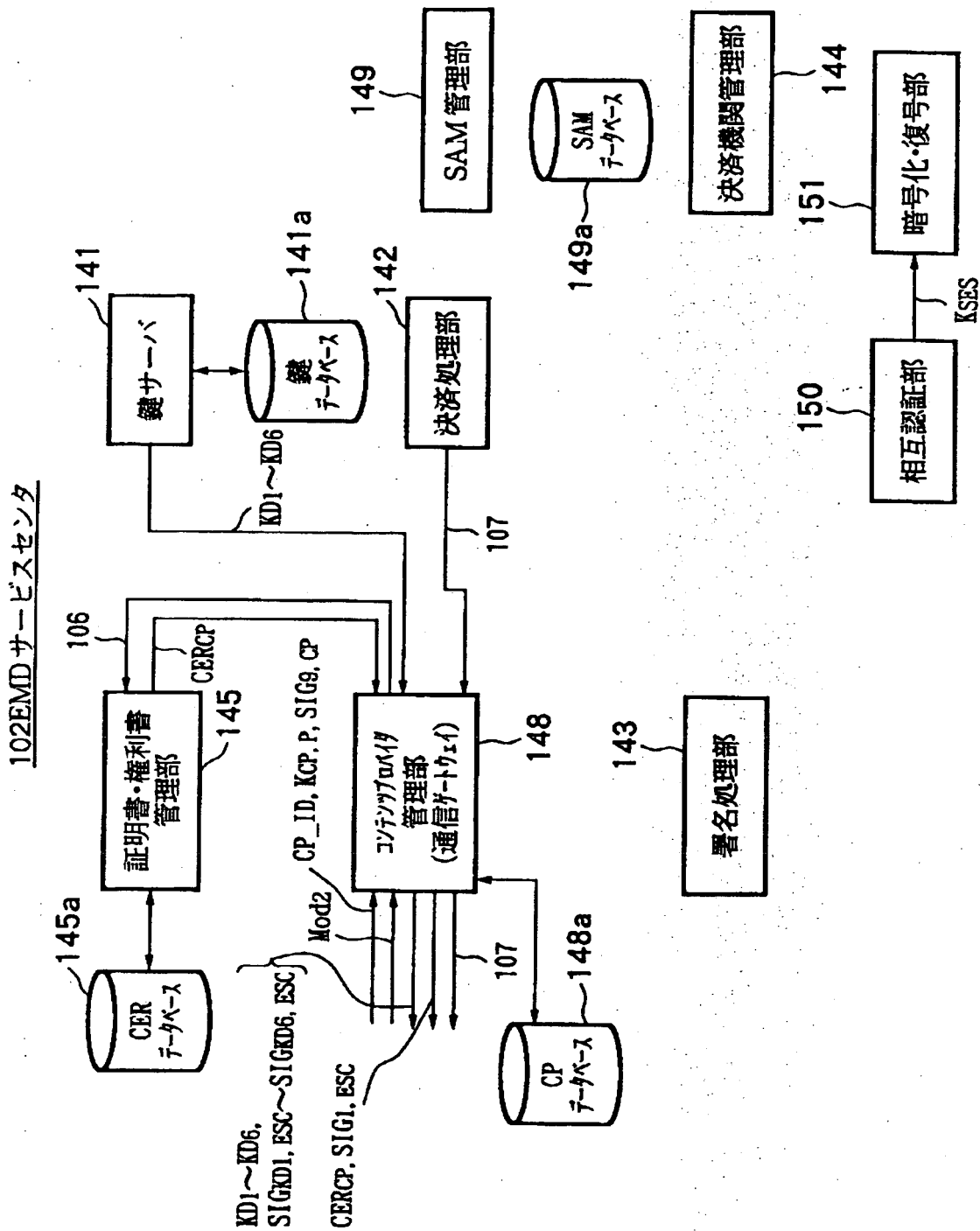
【図 5】



【図 6】

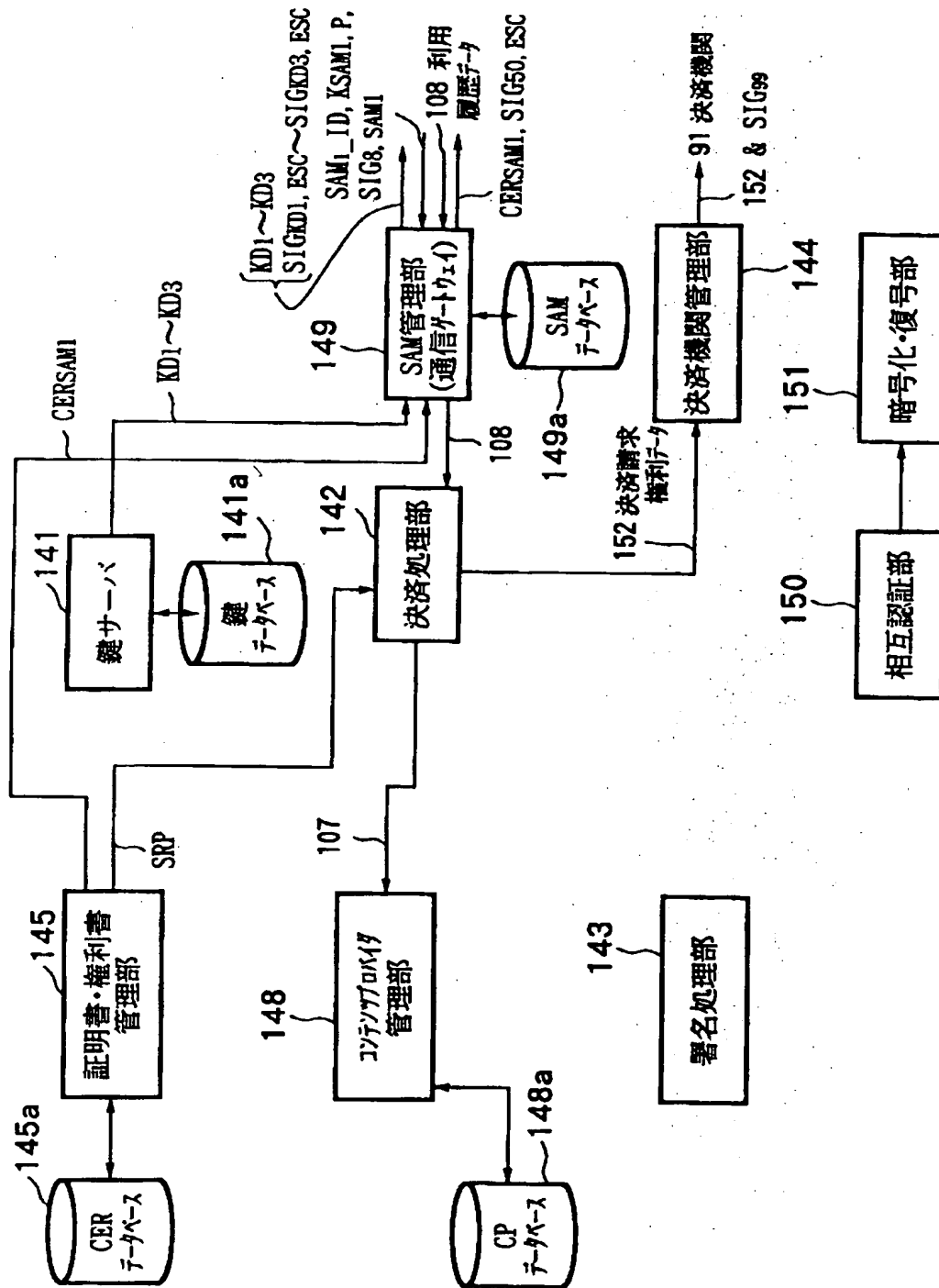


【図 7】

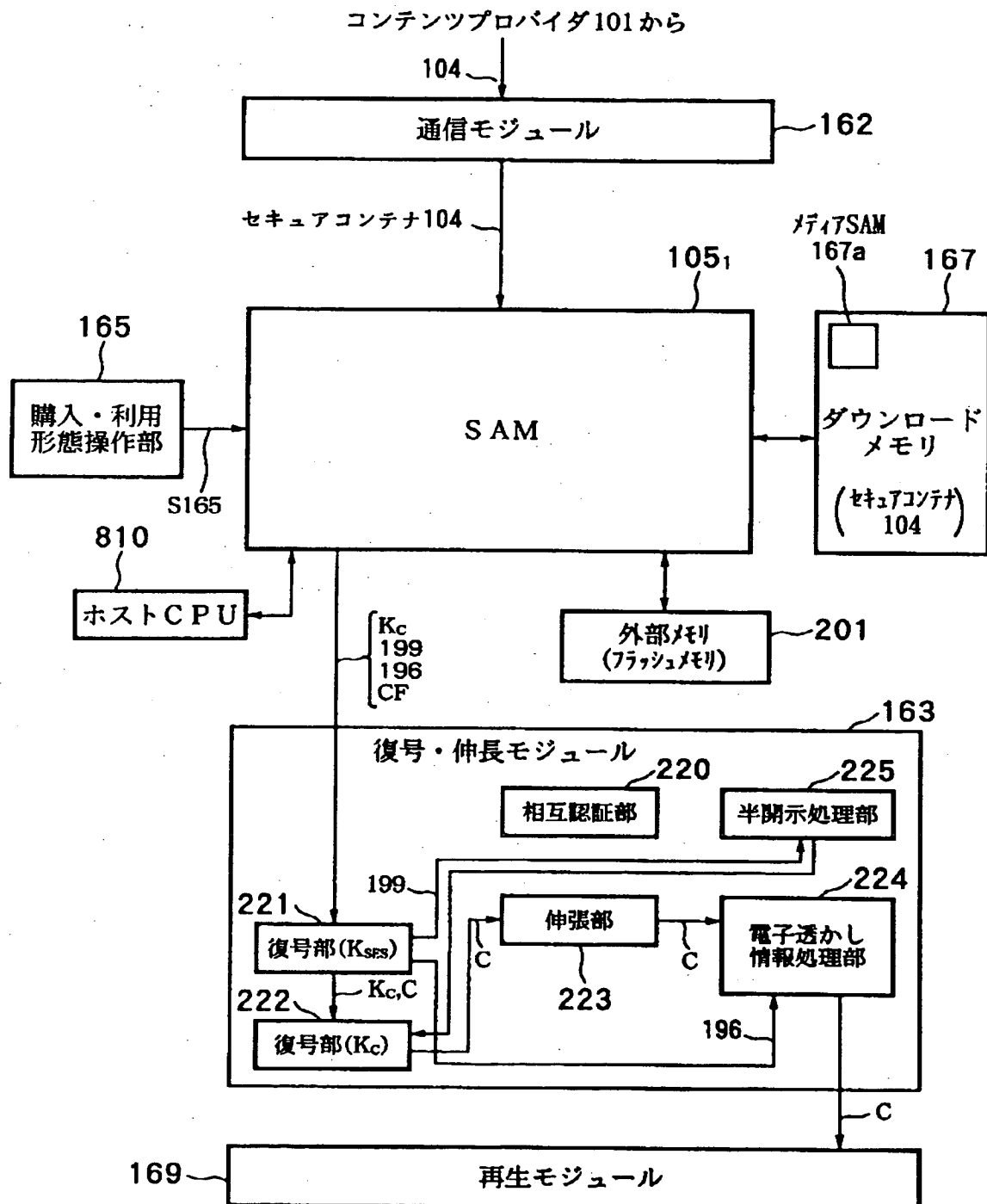


【図 8】

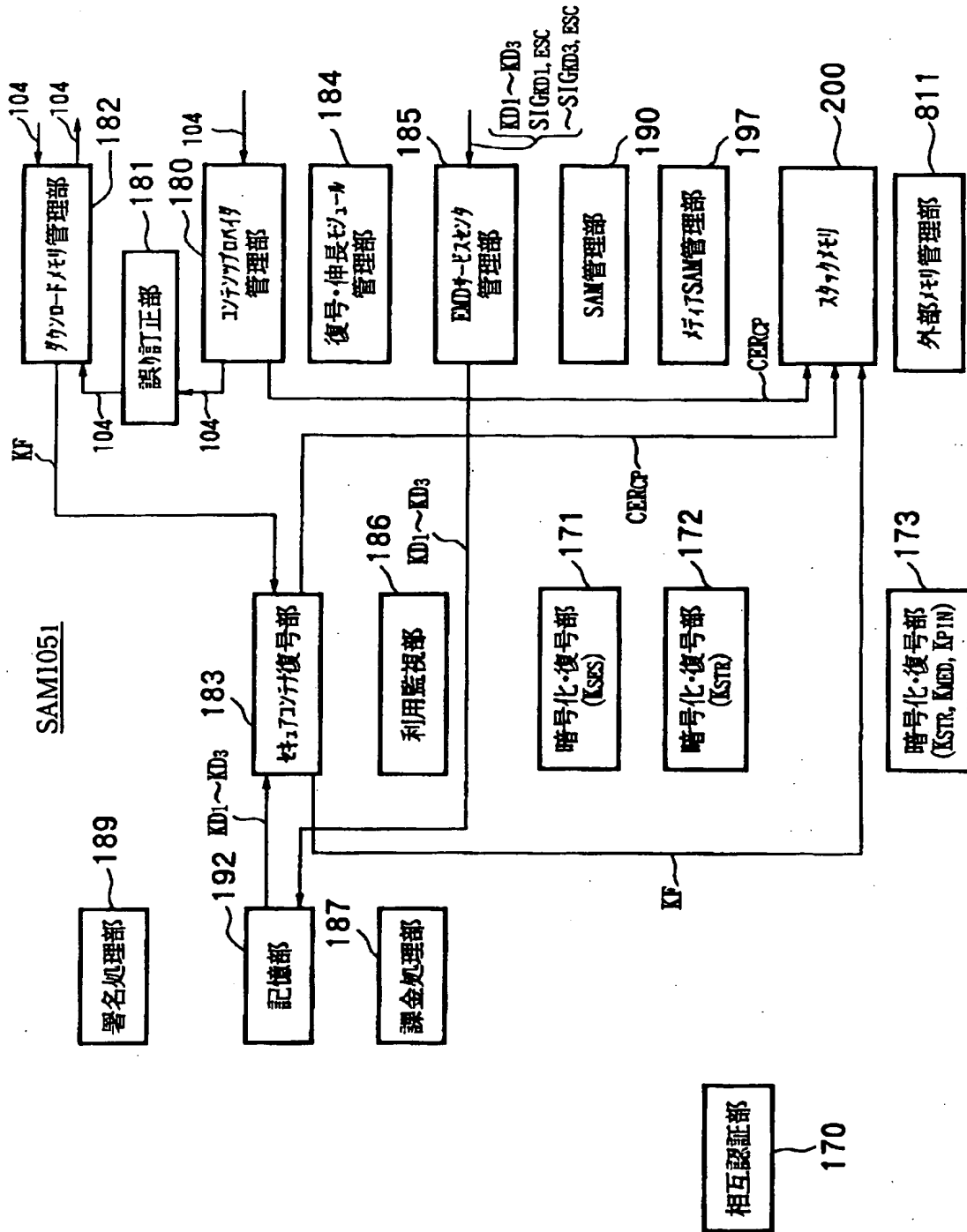
102EMD サービスセンタ



【図 9】



【図 10】



【図 11】

外部メモリ 201 に記憶されるデータ

利用履歴データ 108

SAM 登録リスト

【図 12】

スタックメモリ 200 に記憶されるデータ

コンテンツ鍵データ Kc

権利書データ (UCP) 106

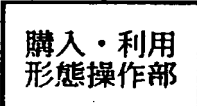
記憶部 (フラッシュメモリ) 192 のロック鍵データ K_{Loc}

コンテンツプロバイダ 101 の公開鍵証明書 CER_{Cp}

利用制御情状態データ (UCS) 166

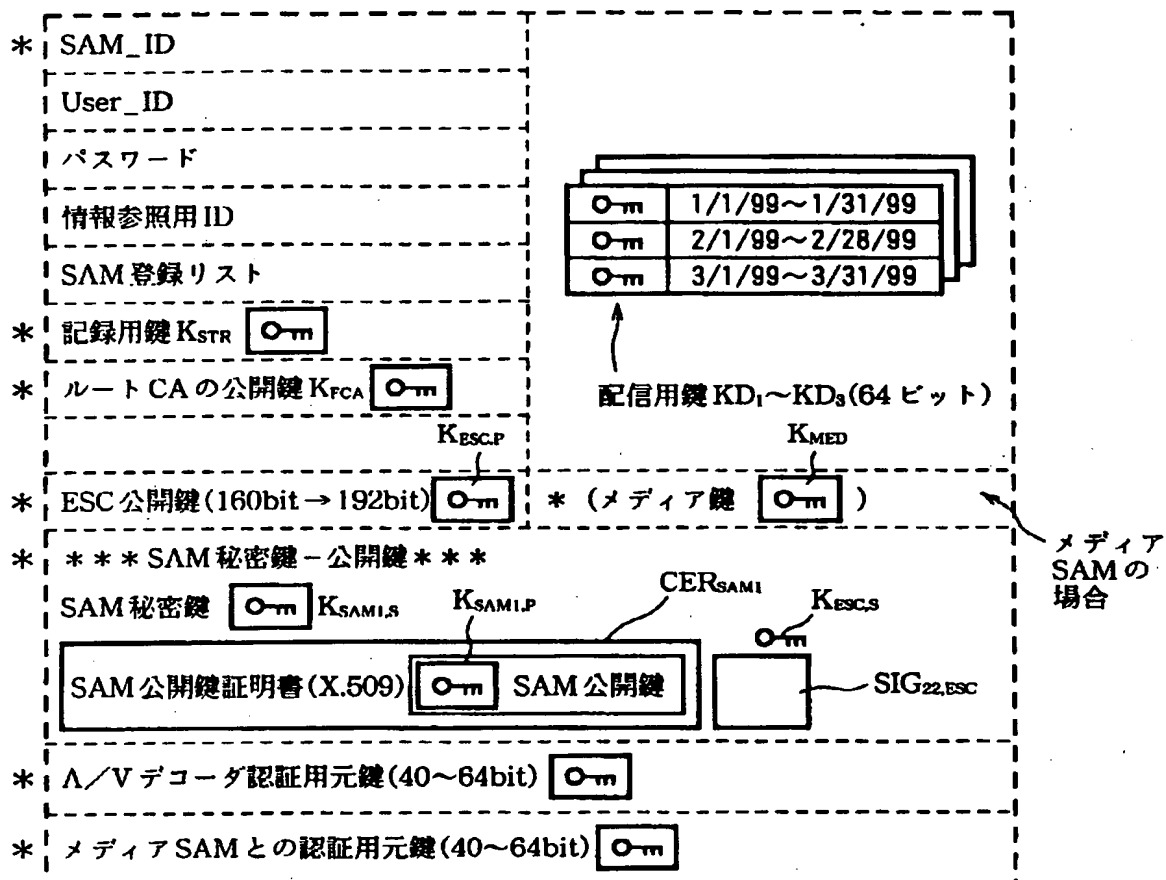
SAM プログラム・ダウンロード・コンテナ SD₁~SD₃

購入・利用
形態操作部

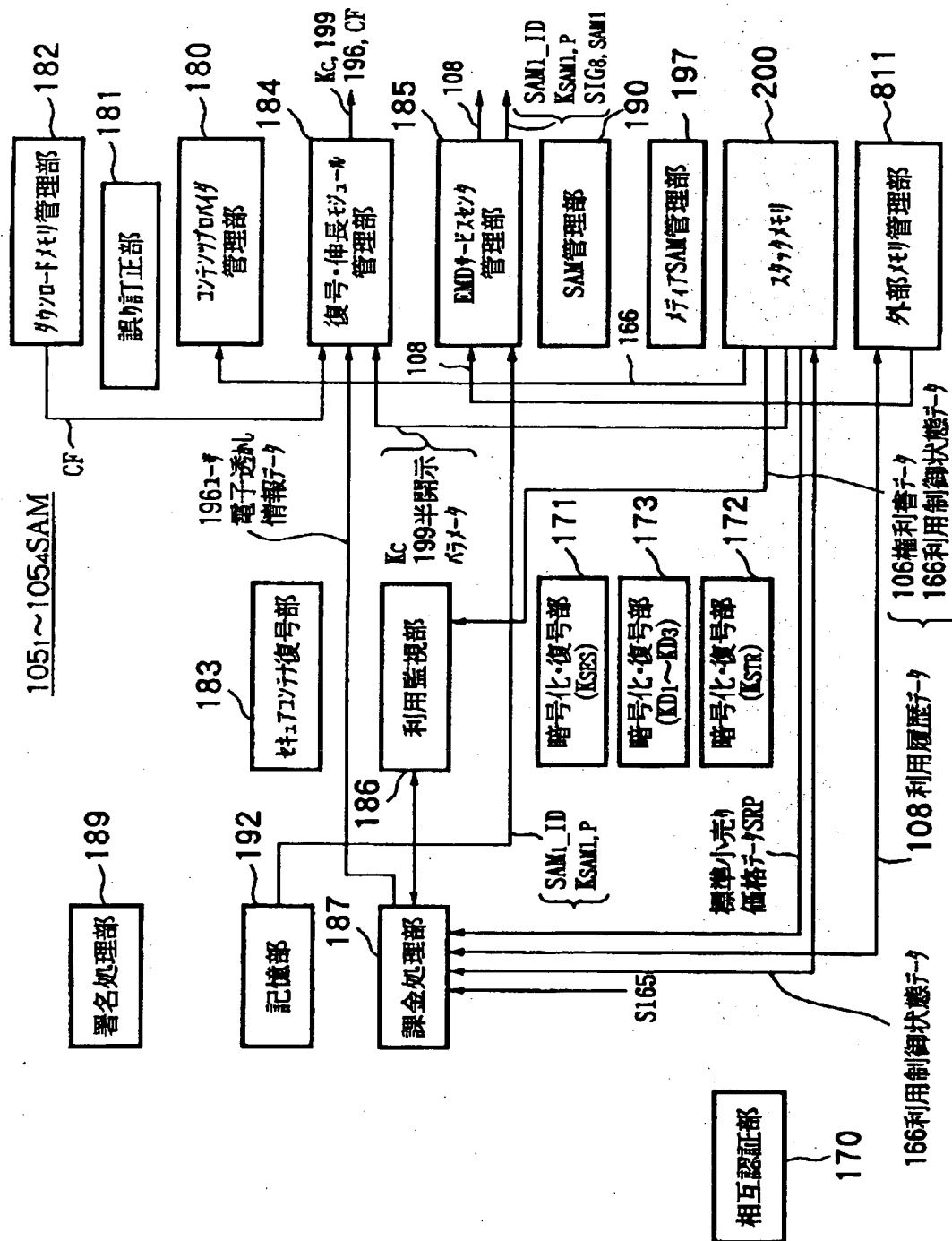


【图 14】

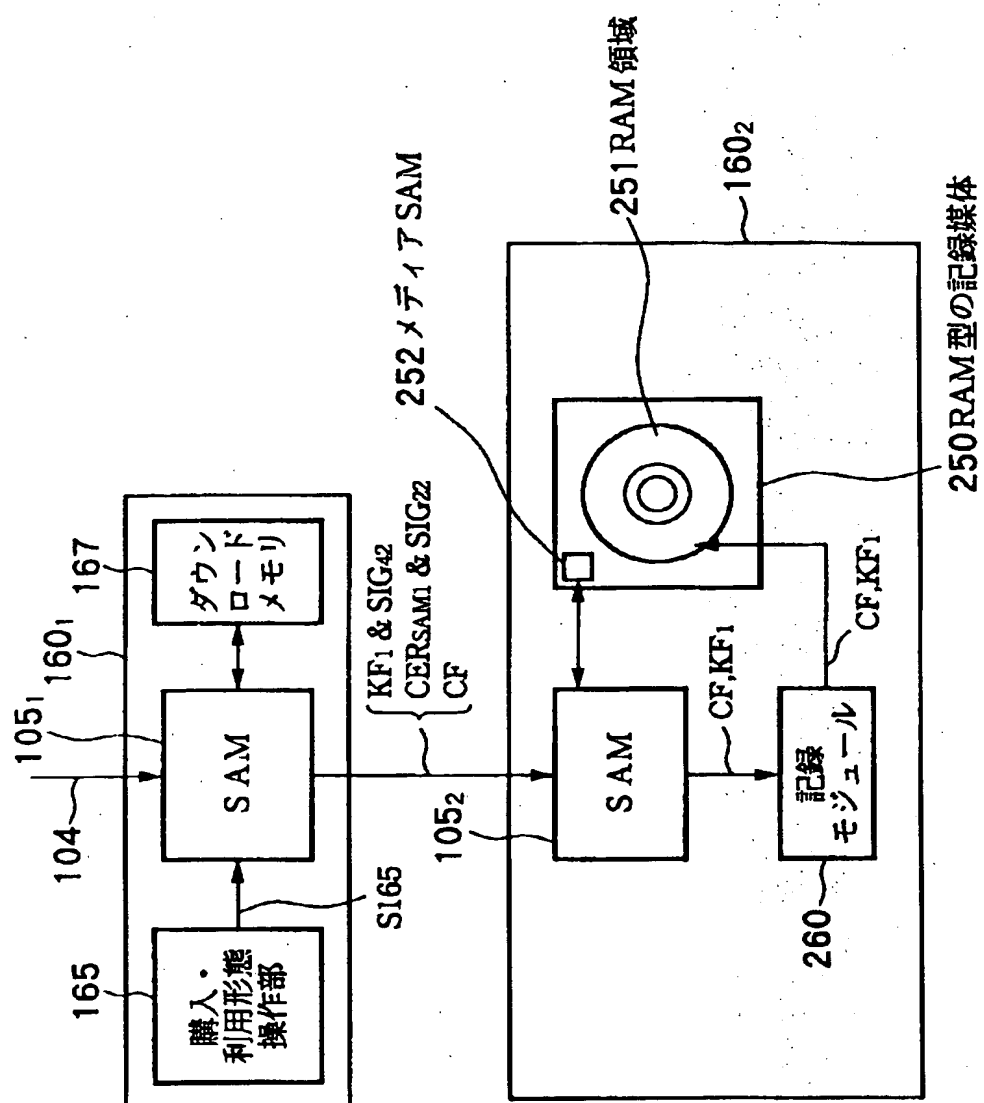
記憶部 192 に記憶されるデータ



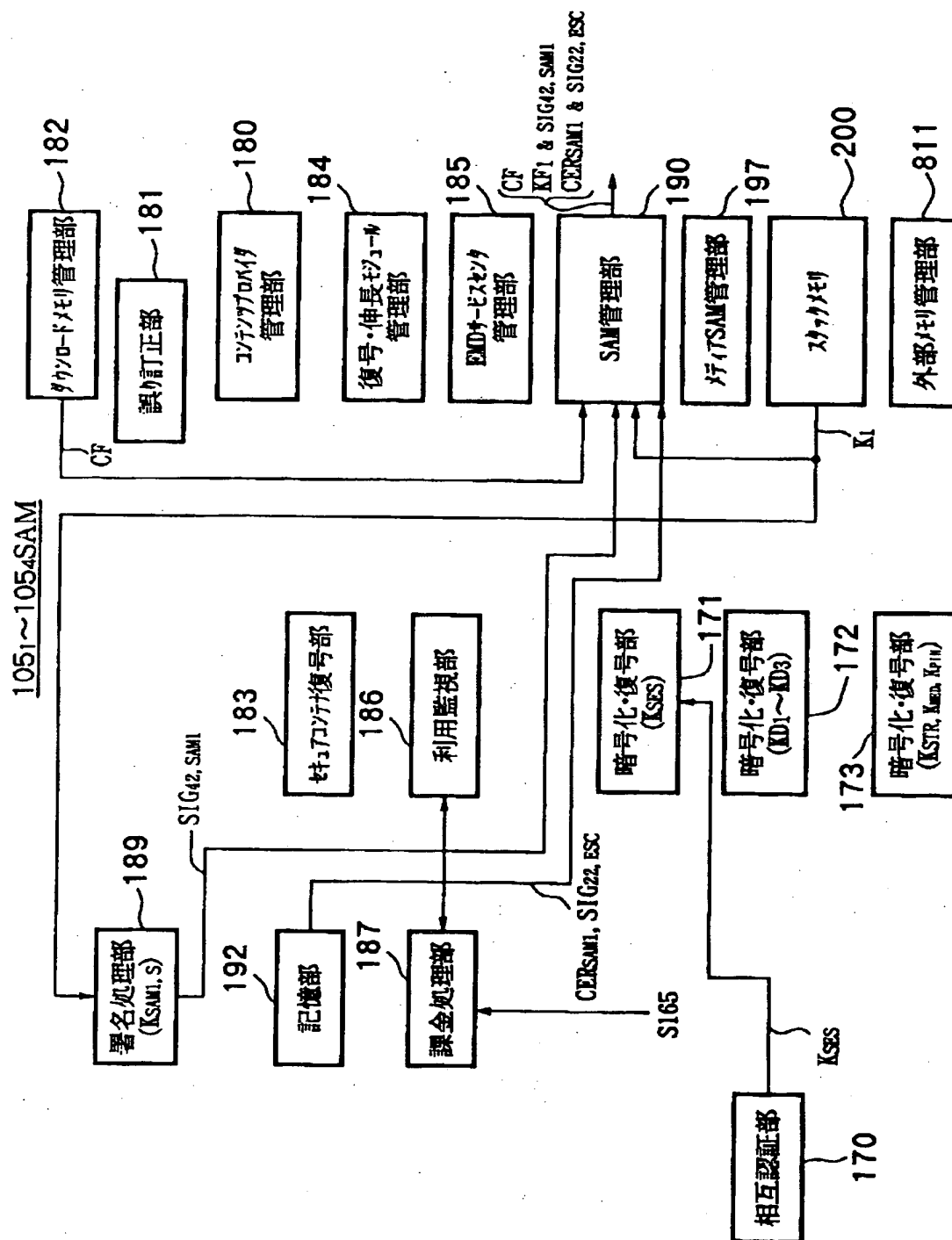
【図 15】



【图 16】

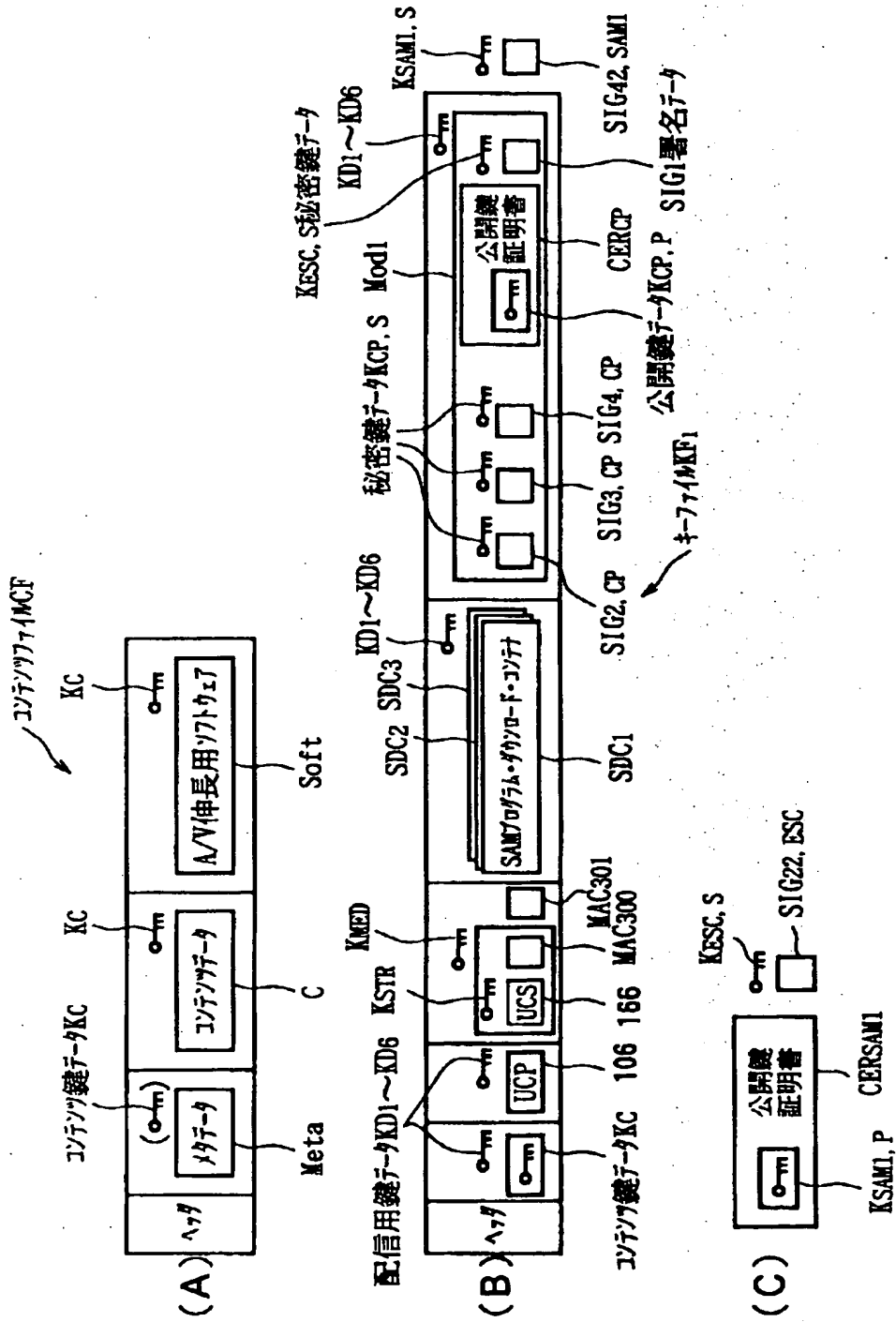


【図 17】



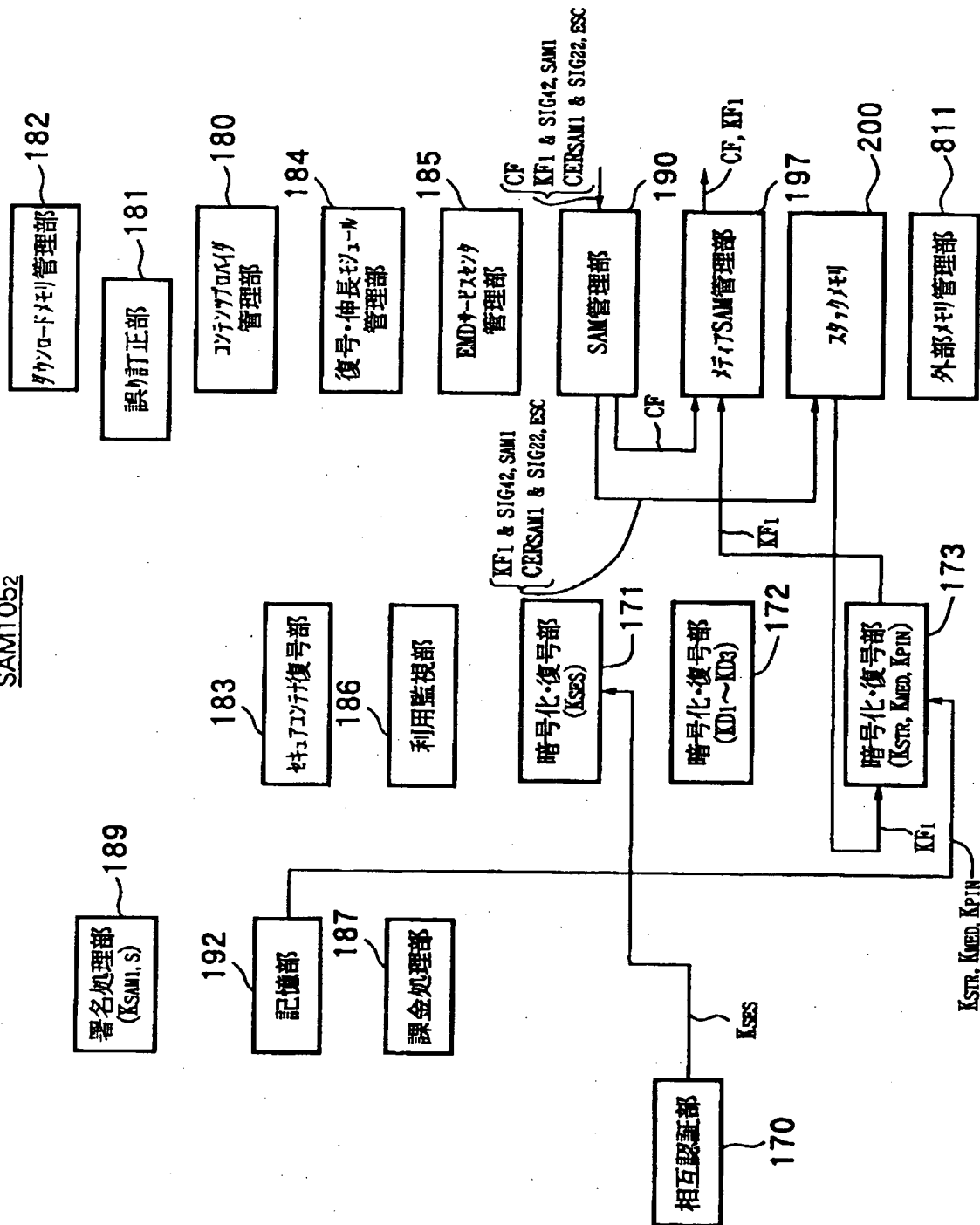
【図 1 8】

購入形態が決定したセキュアコンテナ

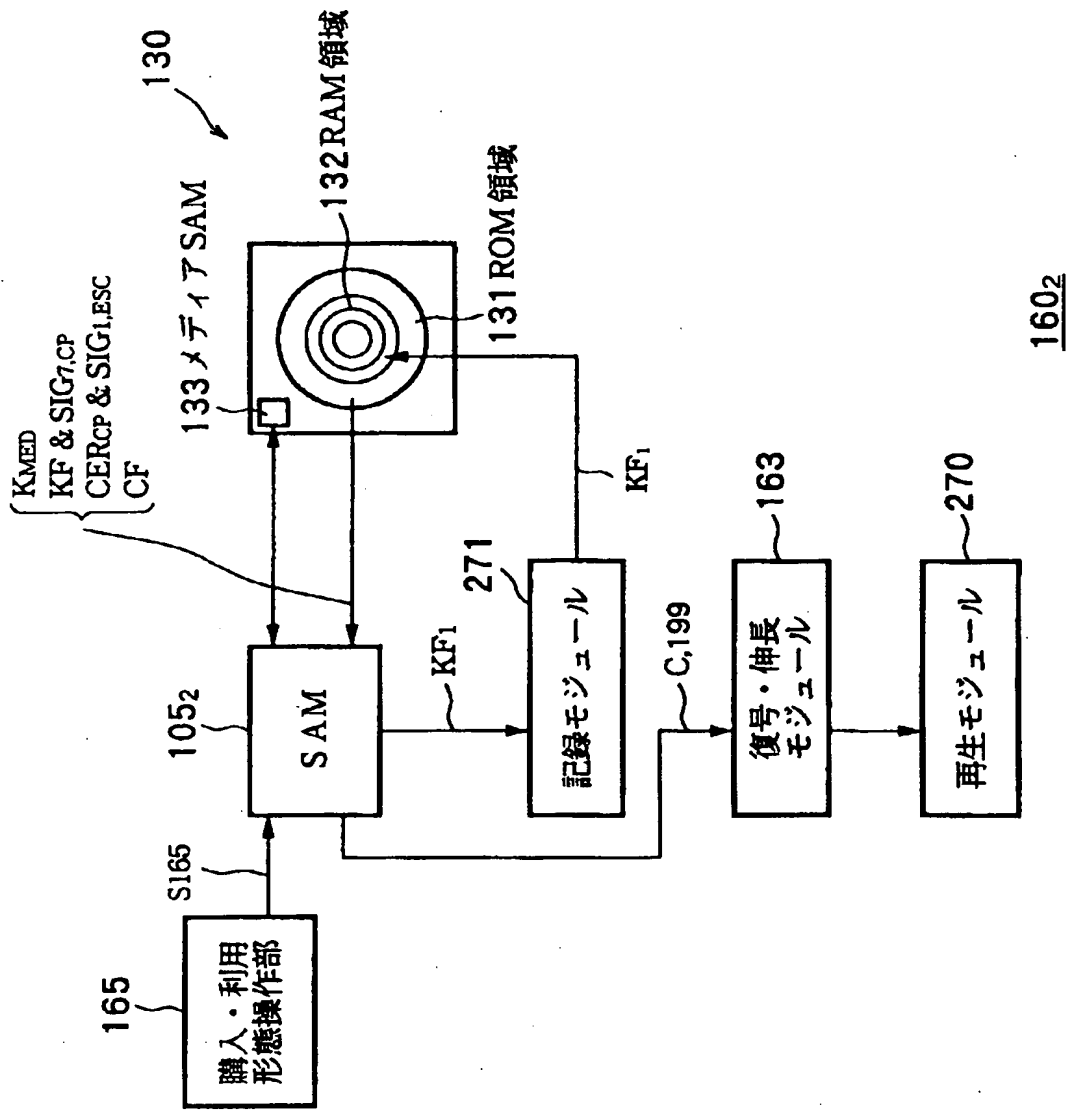


【図 19】

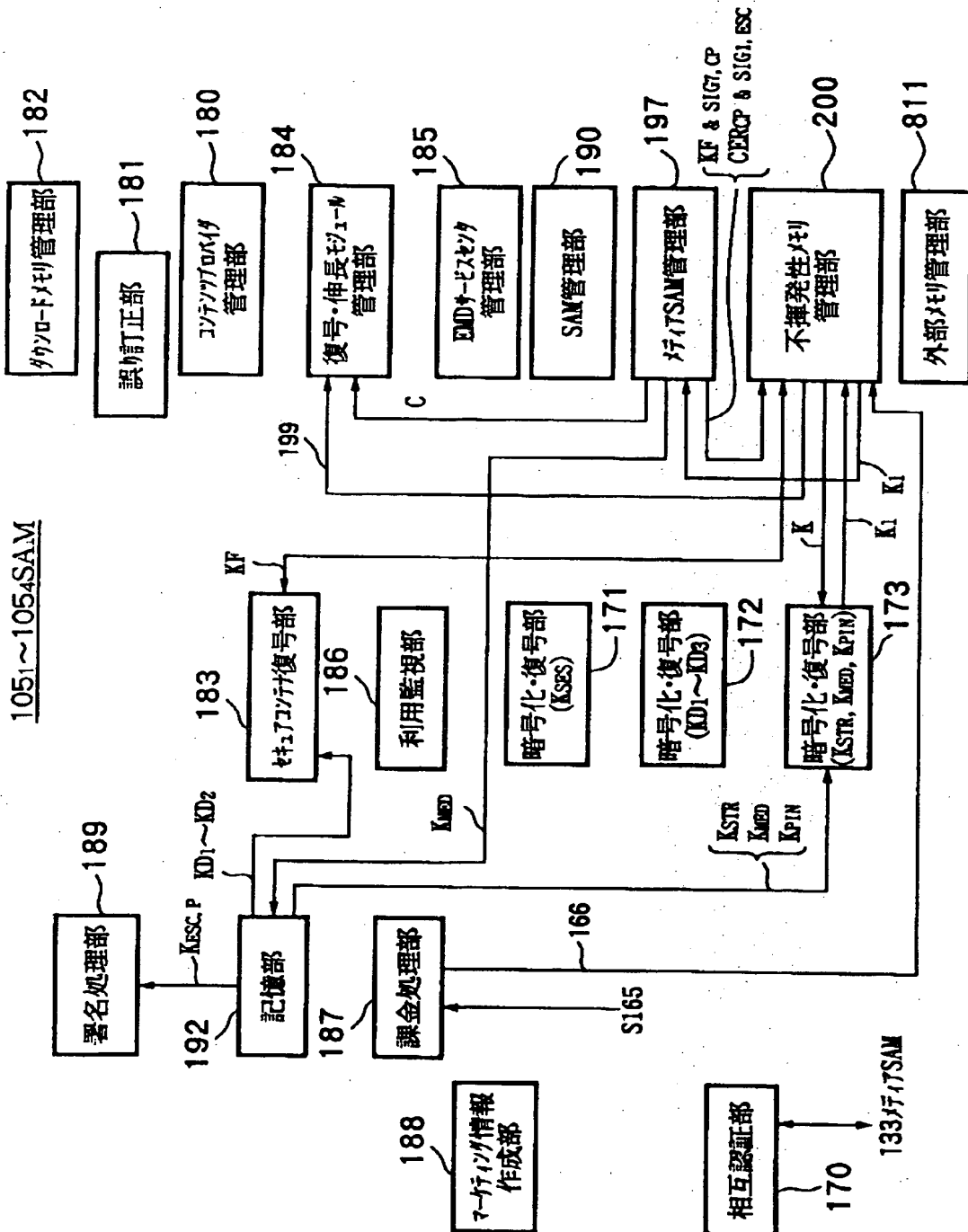
SAM1052



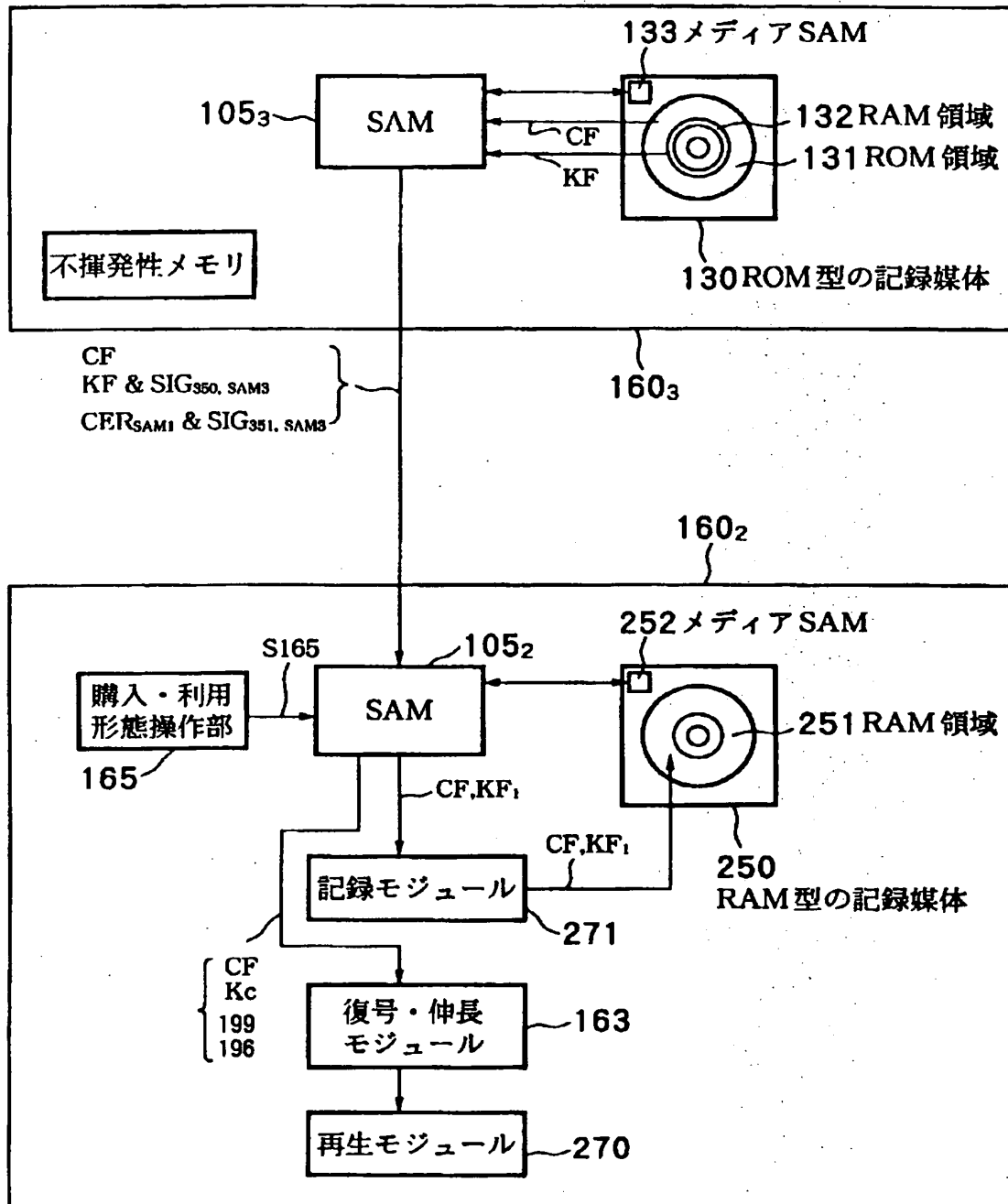
【図 2 0】



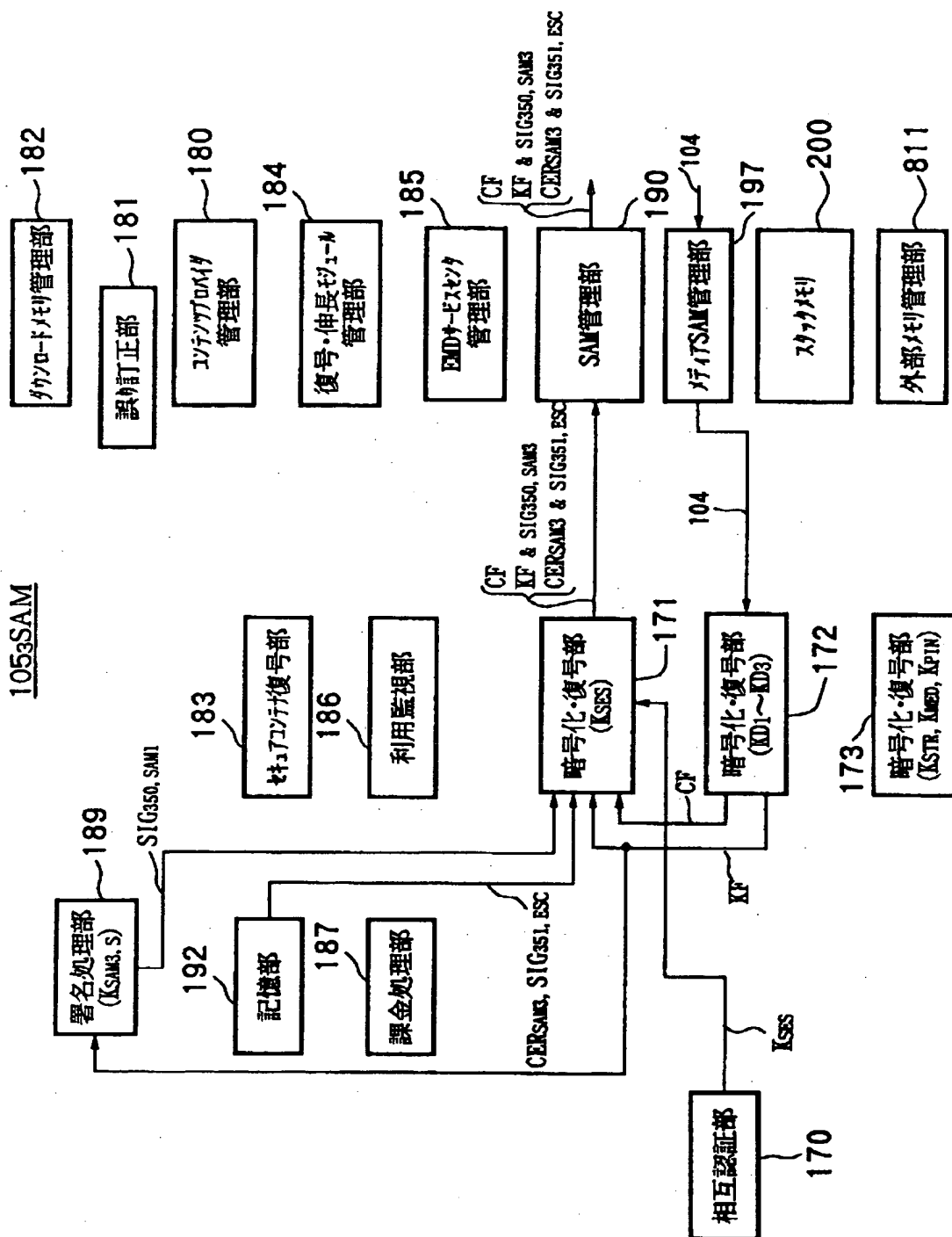
【図 2 1】



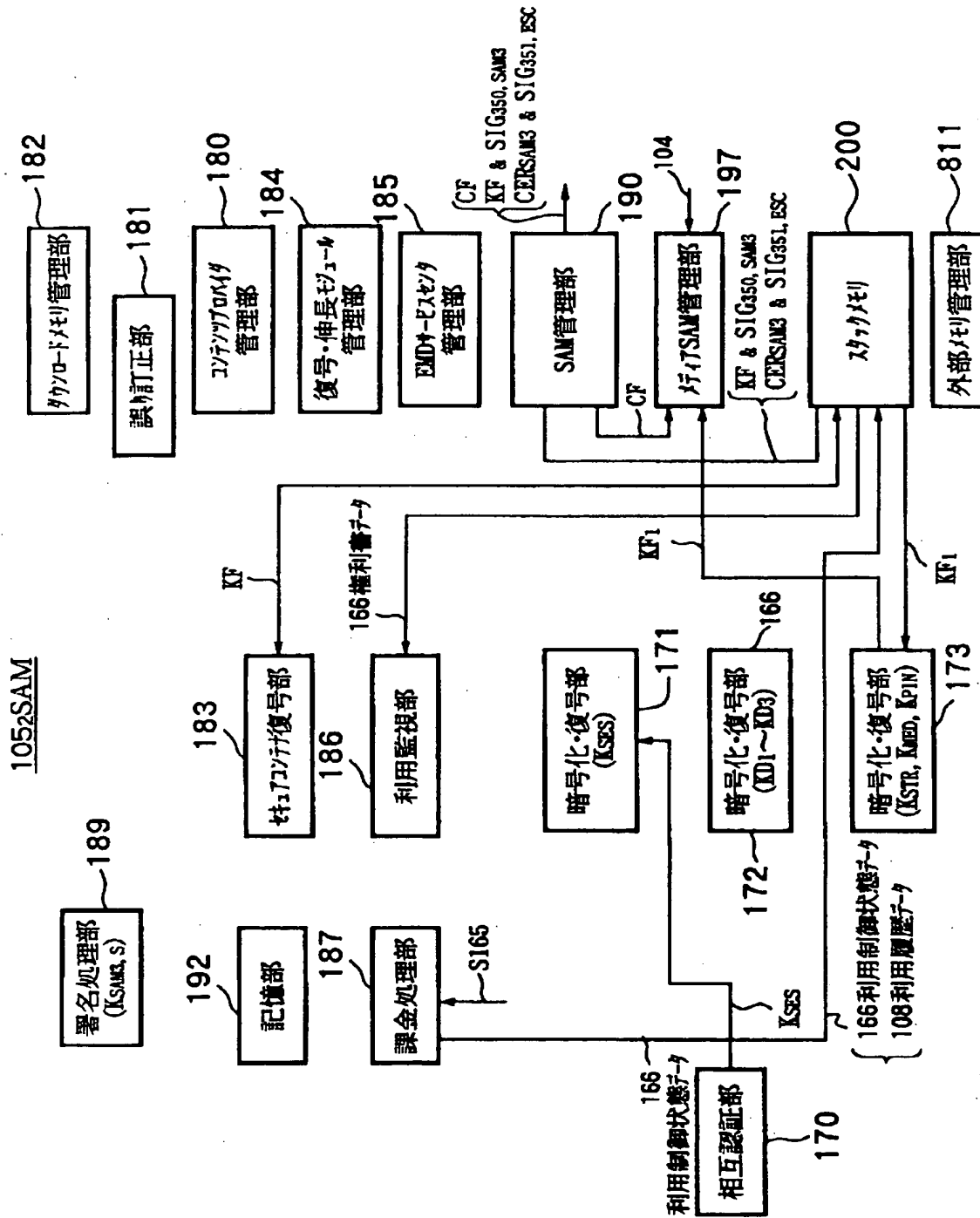
【図 22】



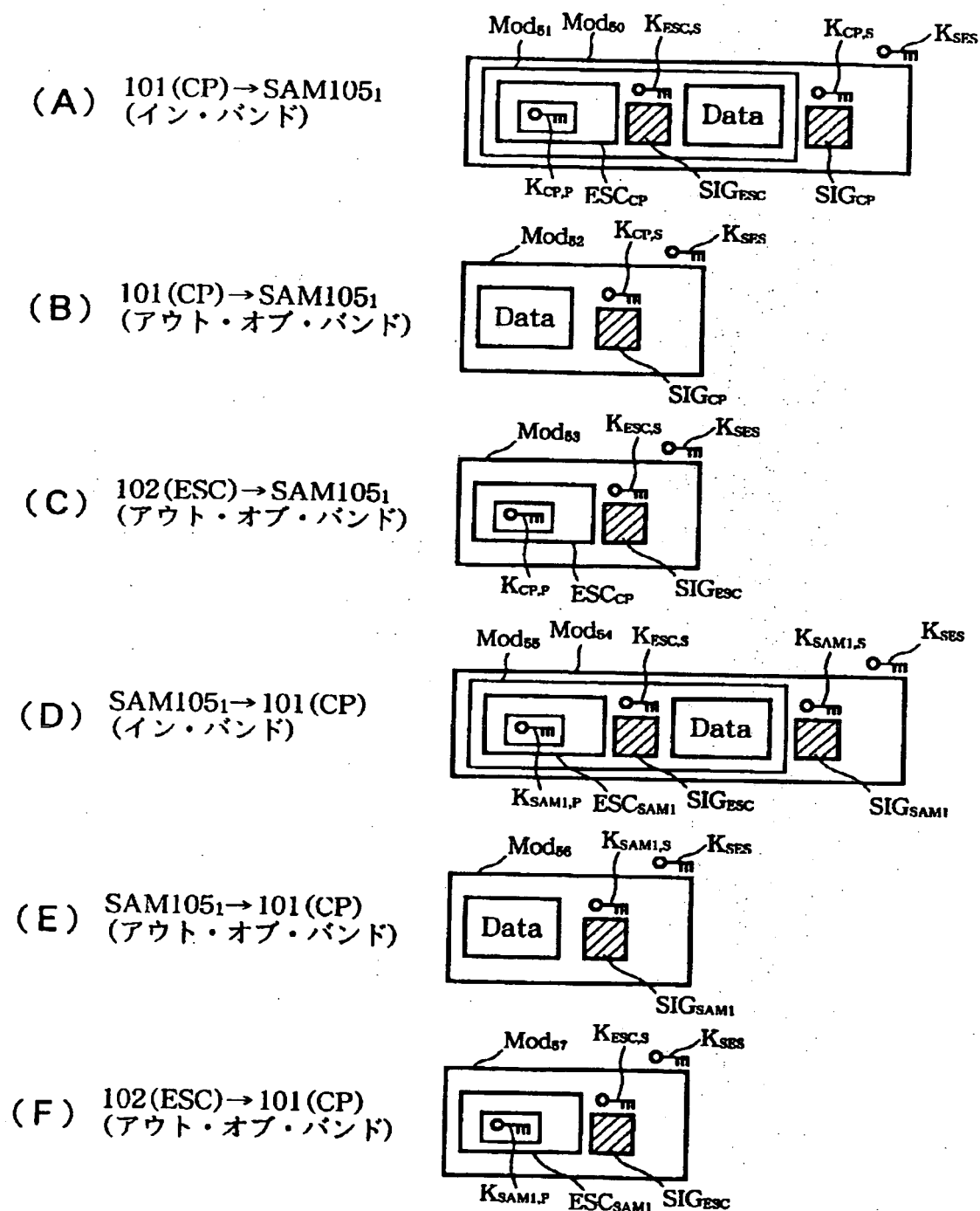
【图 23】



【図 24】

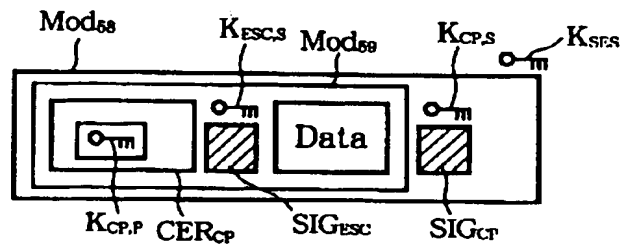


【図 25】

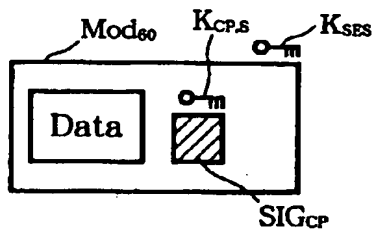


【図 26】

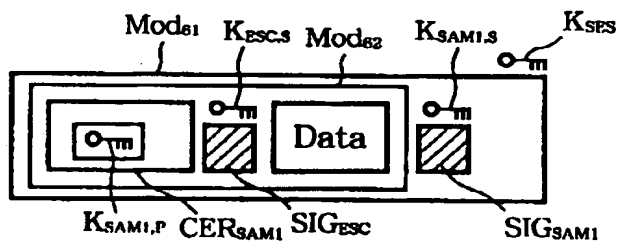
(G) 101 (CP) → 102 (ESC)
(イン・バンド)



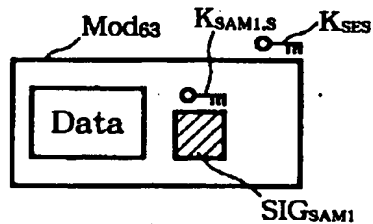
(H) 101 (CP) → 102 (ESC)
(アウト・オブ・バンド)



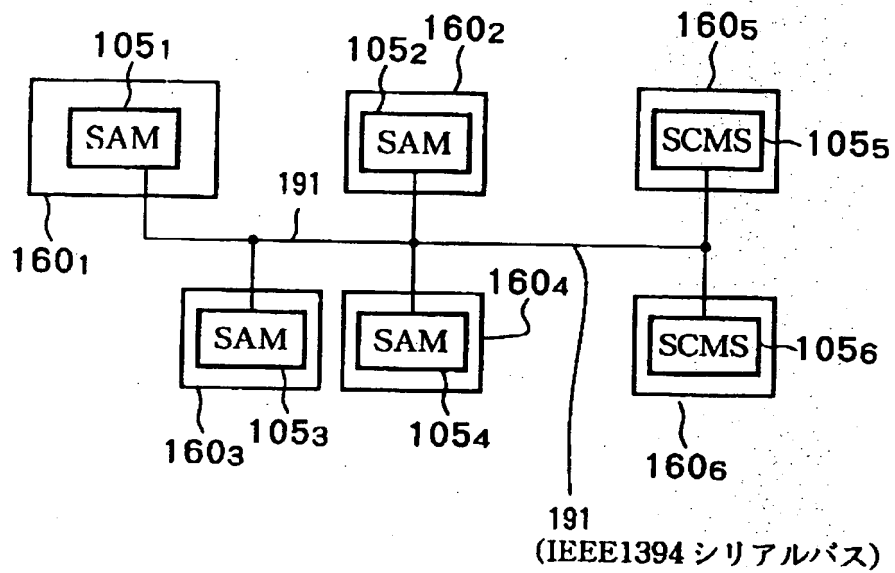
(I) SAM105₁ → 102 (ESC)
(イン・バンド)



(J) SAM105₁ → 102 (ESC)
(アウト・オブ・バンド)



【図 2 7】

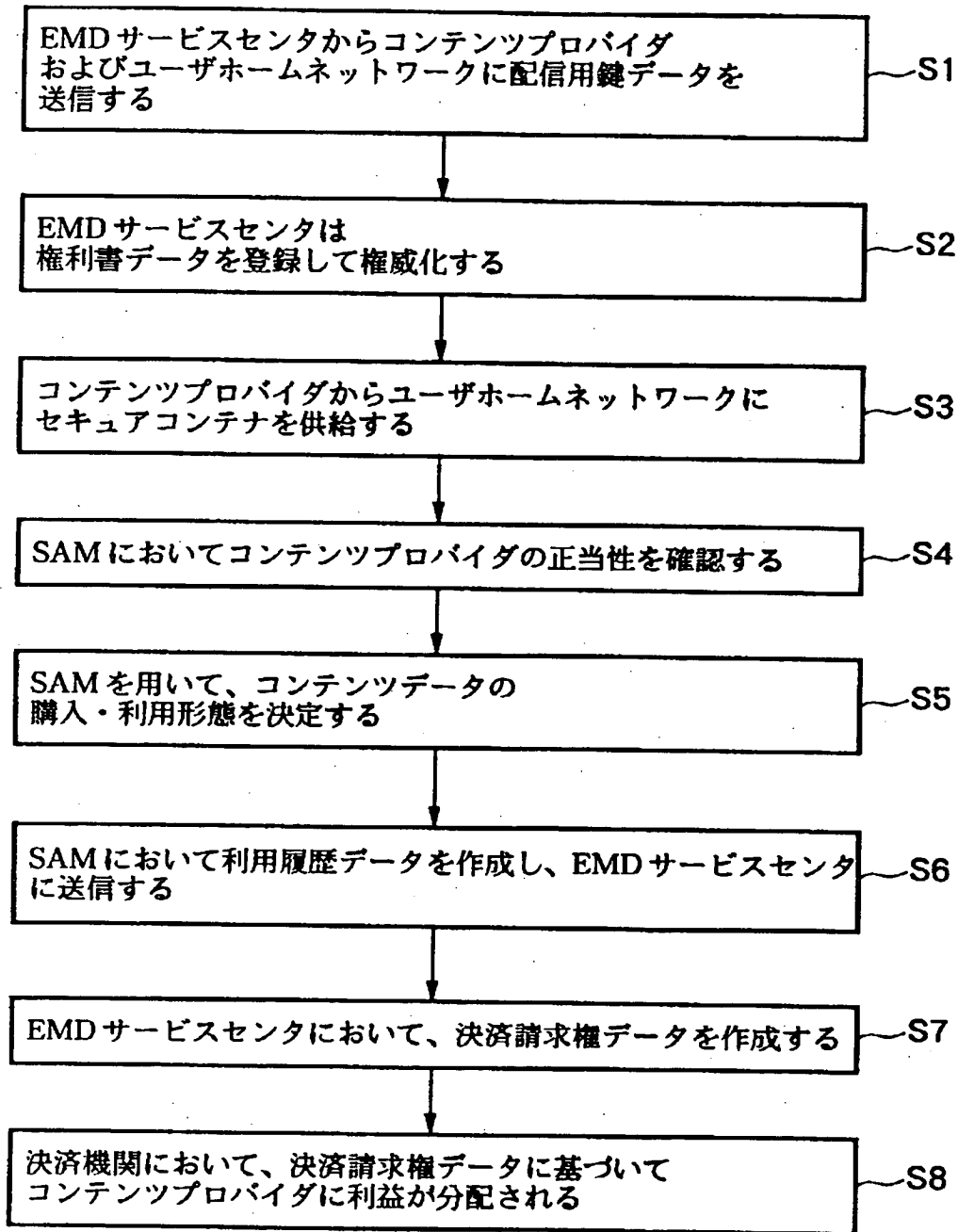


【図 28】

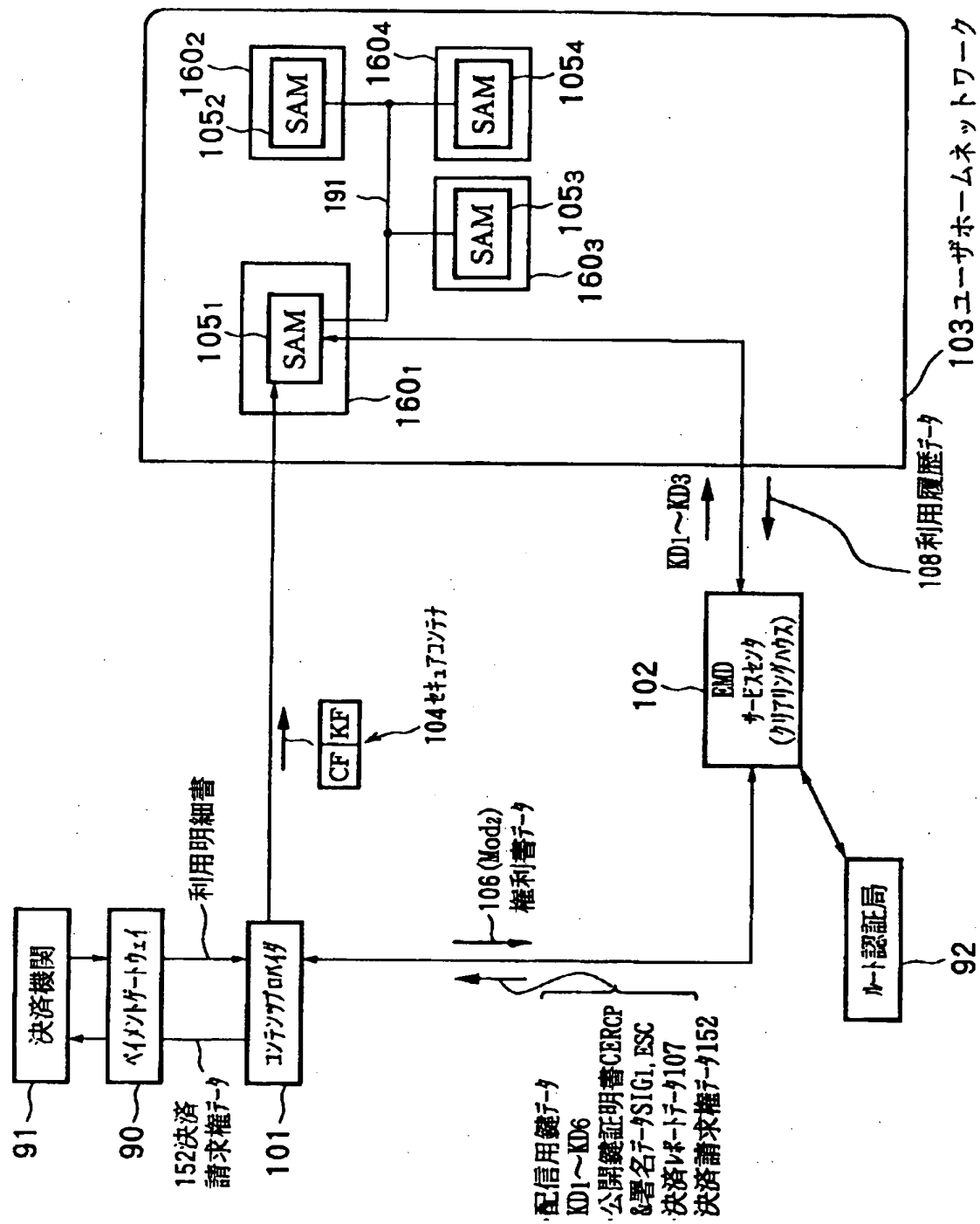
リストを発行した SAM の SAM_ID (Issure_SAM)								
SAM 登録リストの有効期限								
SAM 登録数								
SAM の接続リスト (SAM_ID)								
SAM の決済機能 有/無 (Settlement Function)								
Revocation_Flag その SAM がリボークされているか。								
各々の SAM の公開鍵								
ESC 秘密鍵による署名データ								
<table border="1"> <tr> <td>ハッシュ関数</td> </tr> <tr> <td>リストを発行した SAM の SAM_ID (Issure_SAM)</td> </tr> <tr> <td>Registration List の有効期限</td> </tr> <tr> <td>SAM 登録数</td> </tr> <tr> <td>SAM の接続リスト (SAM_ID)</td> </tr> <tr> <td>SAM の決済機能 有/無 (Settlement Function)</td> </tr> <tr> <td>Revocation_Flag その SAM がリボークされているか。</td> </tr> <tr> <td>各々の SAM の公開鍵</td> </tr> </table>	ハッシュ関数	リストを発行した SAM の SAM_ID (Issure_SAM)	Registration List の有効期限	SAM 登録数	SAM の接続リスト (SAM_ID)	SAM の決済機能 有/無 (Settlement Function)	Revocation_Flag その SAM がリボークされているか。	各々の SAM の公開鍵
ハッシュ関数								
リストを発行した SAM の SAM_ID (Issure_SAM)								
Registration List の有効期限								
SAM 登録数								
SAM の接続リスト (SAM_ID)								
SAM の決済機能 有/無 (Settlement Function)								
Revocation_Flag その SAM がリボークされているか。								
各々の SAM の公開鍵								

SAM 登録リスト

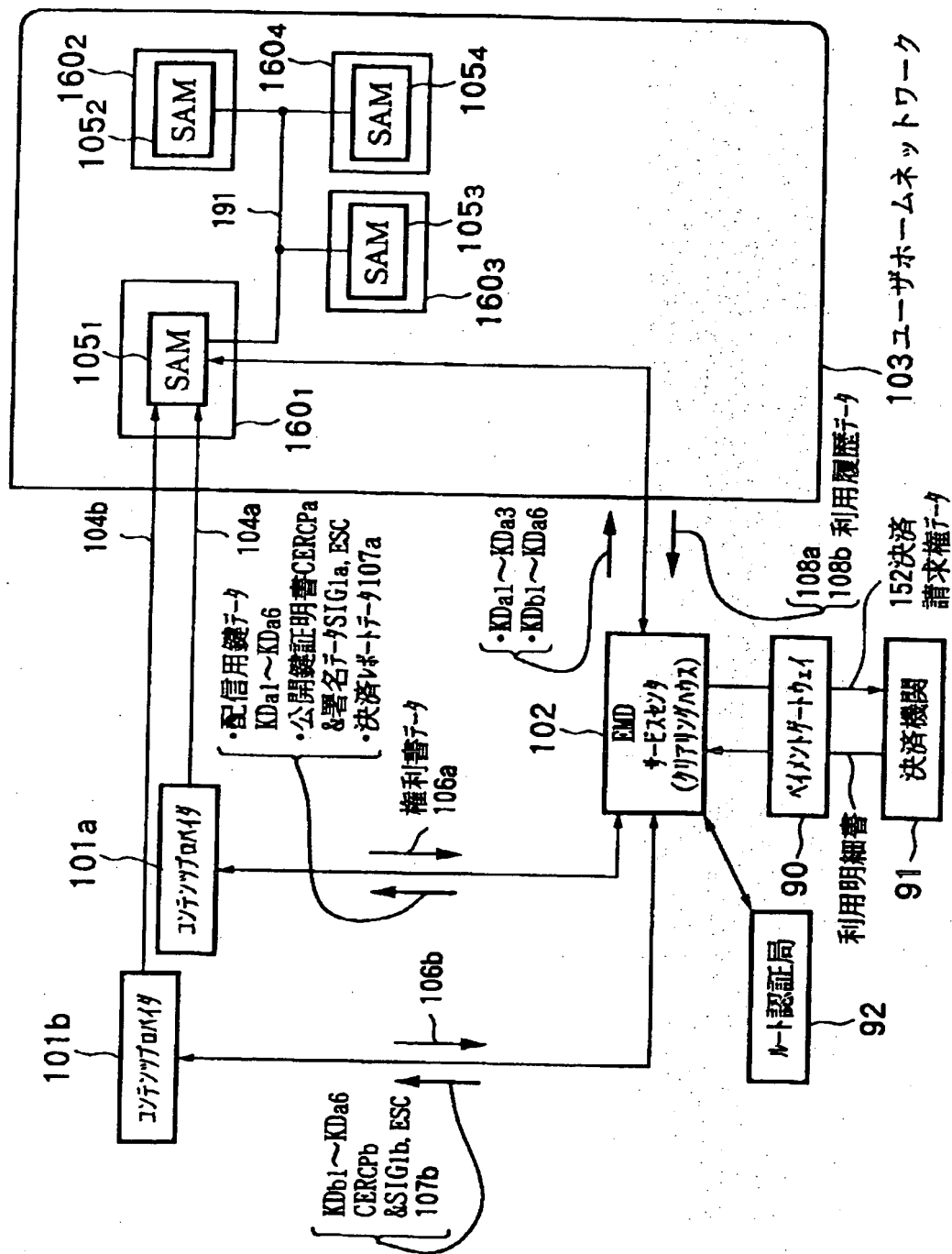
【図 29】



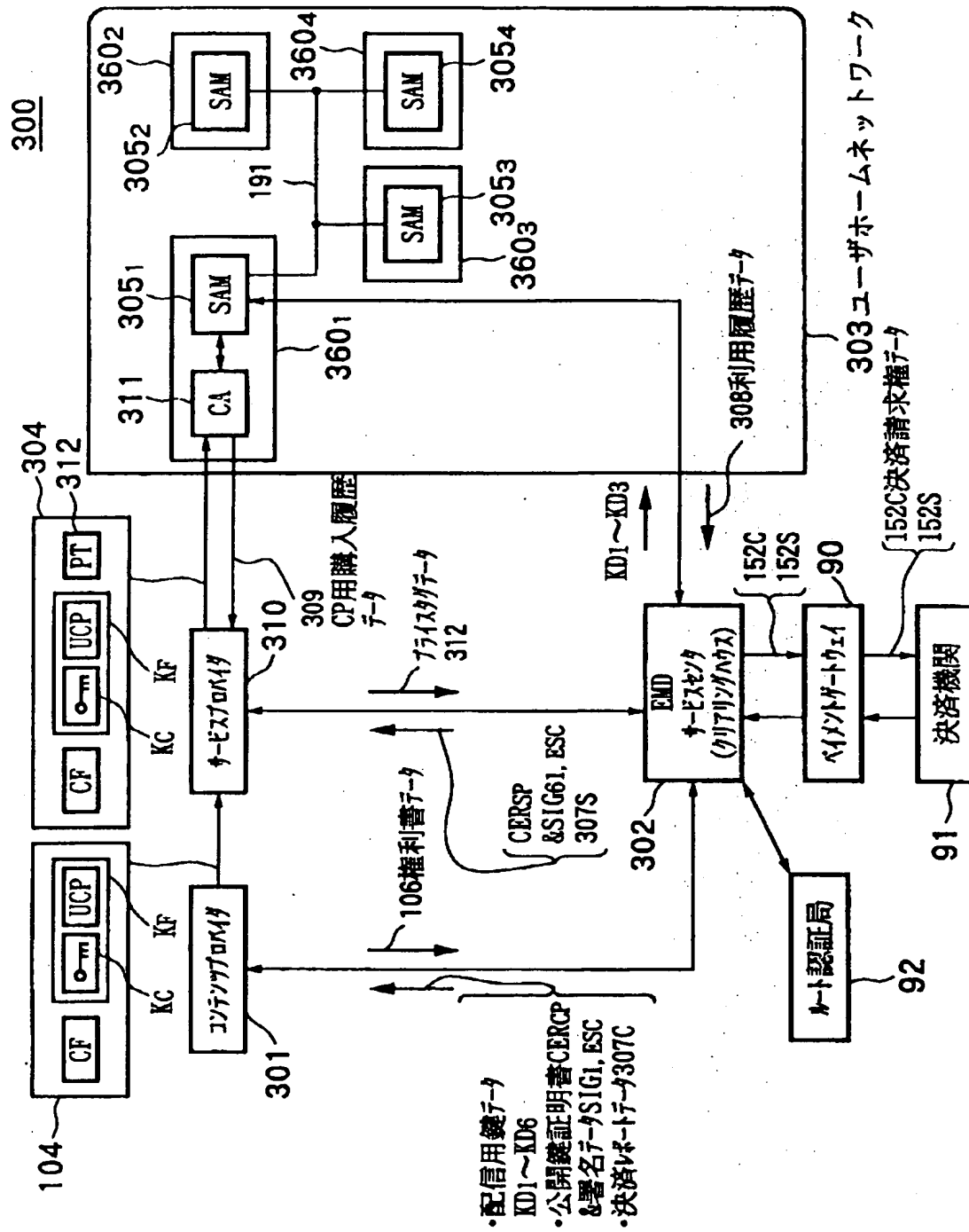
【図 30】



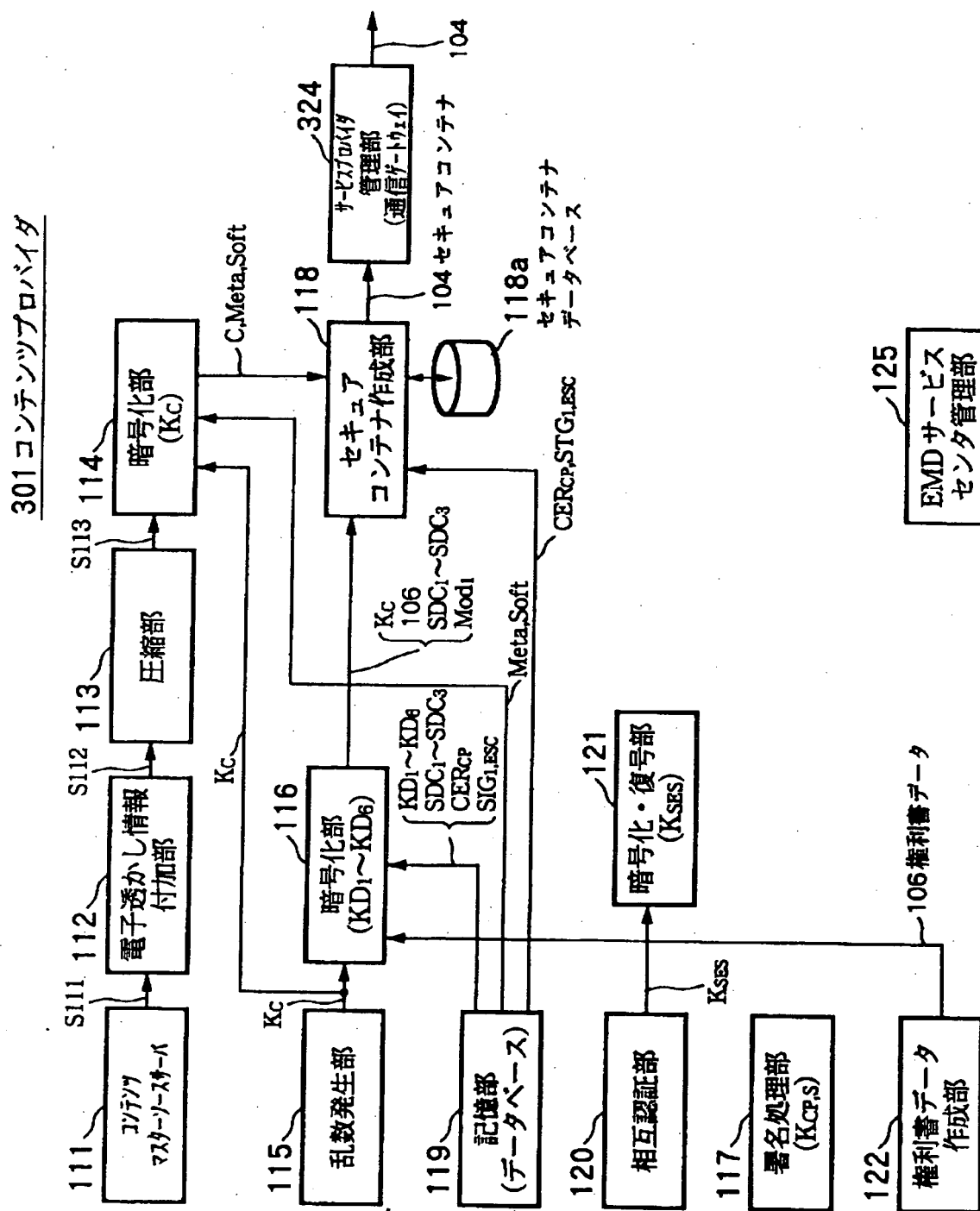
【図 31】



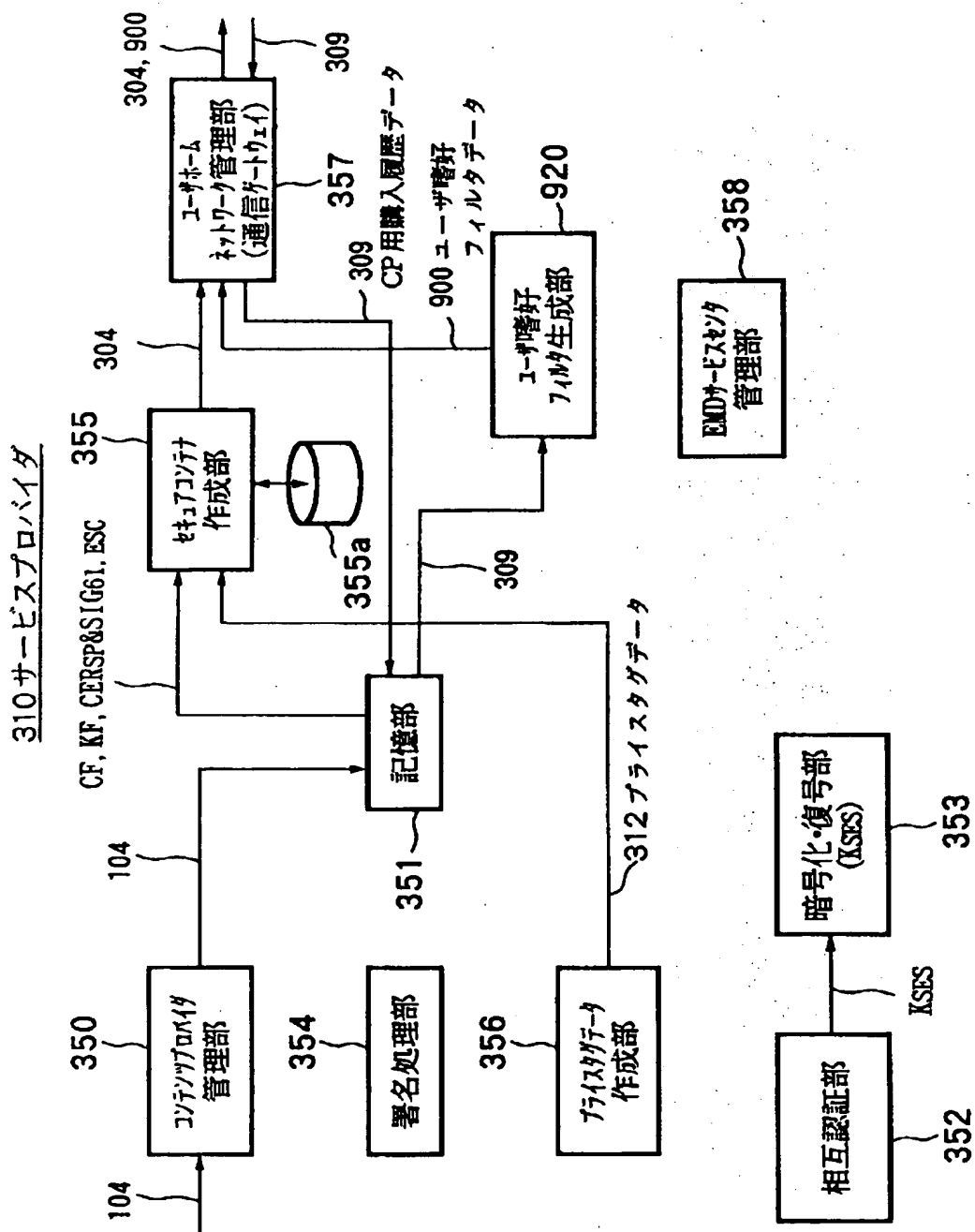
【図 3 2】



【図 3 3】

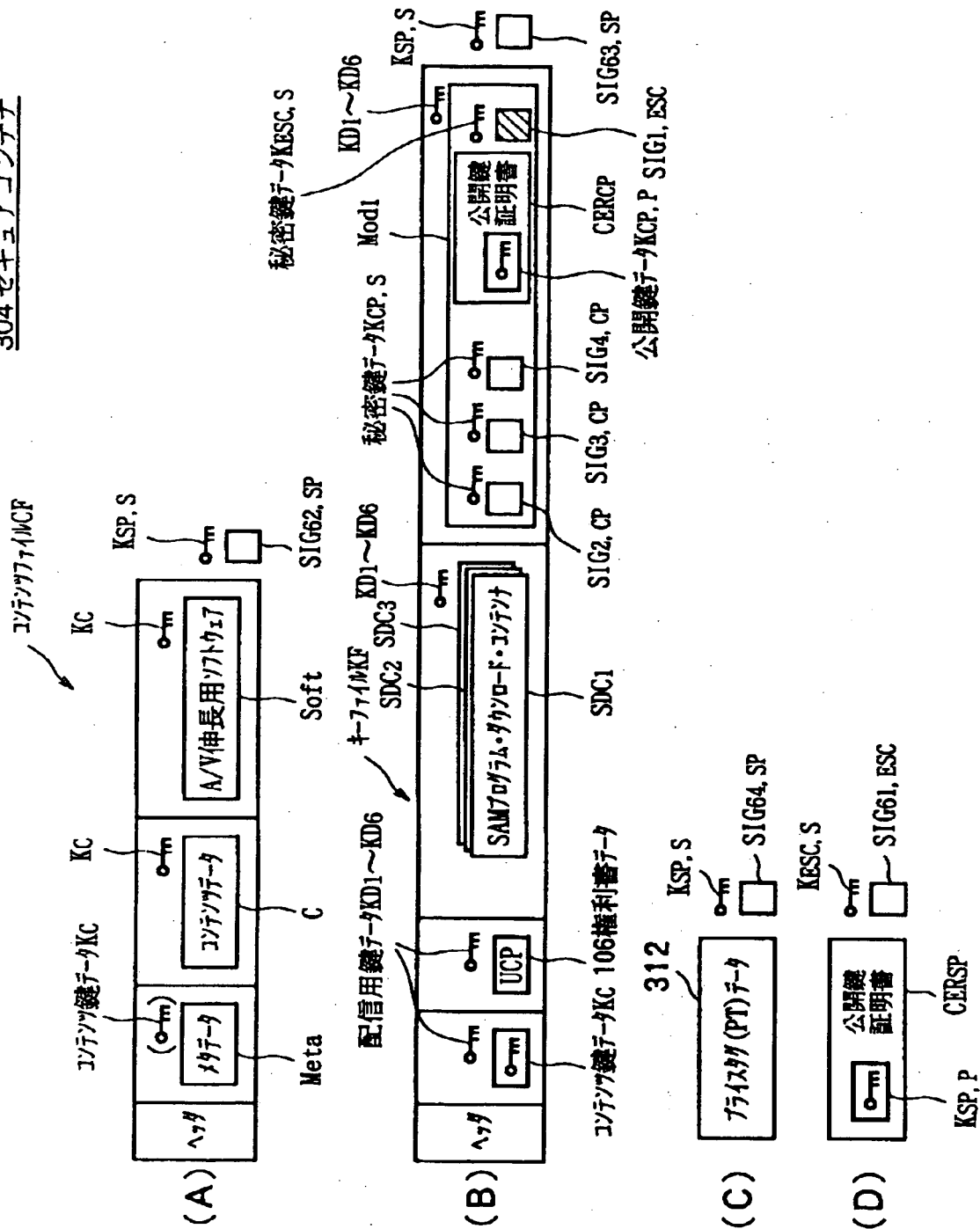


【図 3 4】



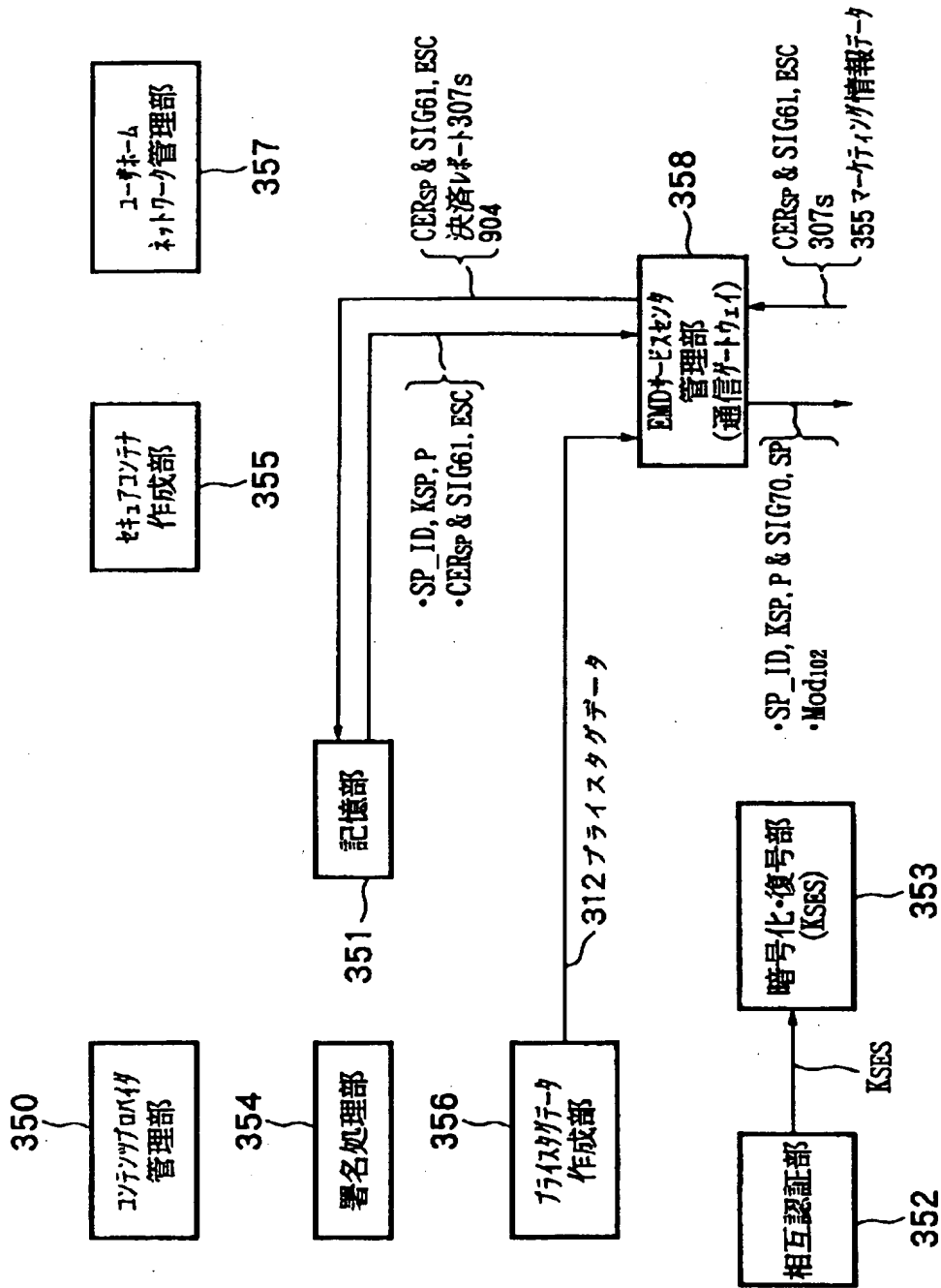
【図 3 5】

304 セキュアコンテナ

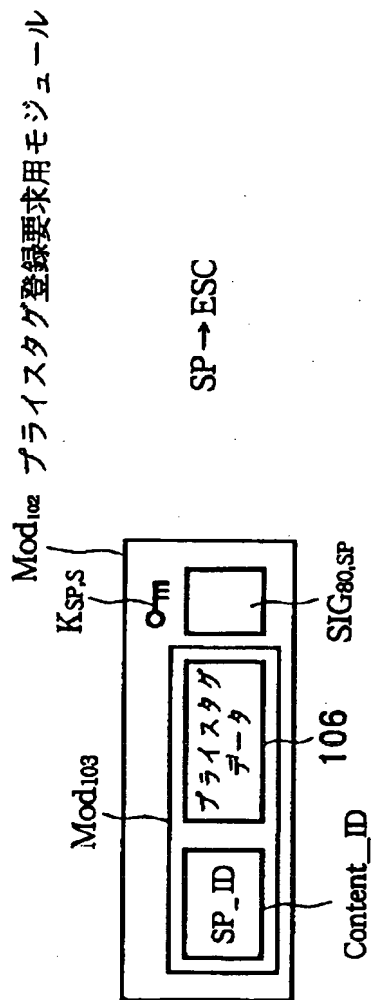


【図 3 6】

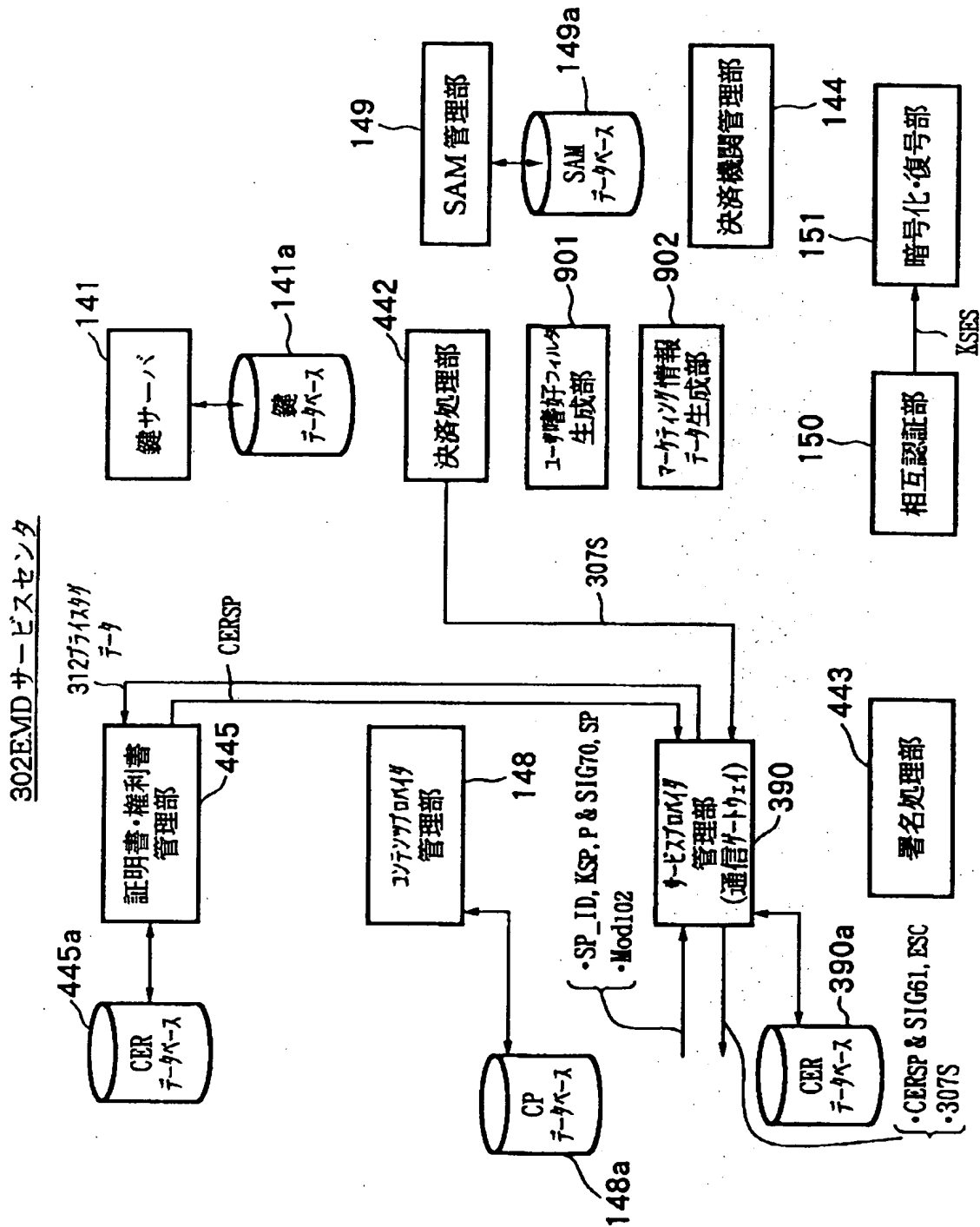
310 サービスプロバイダ



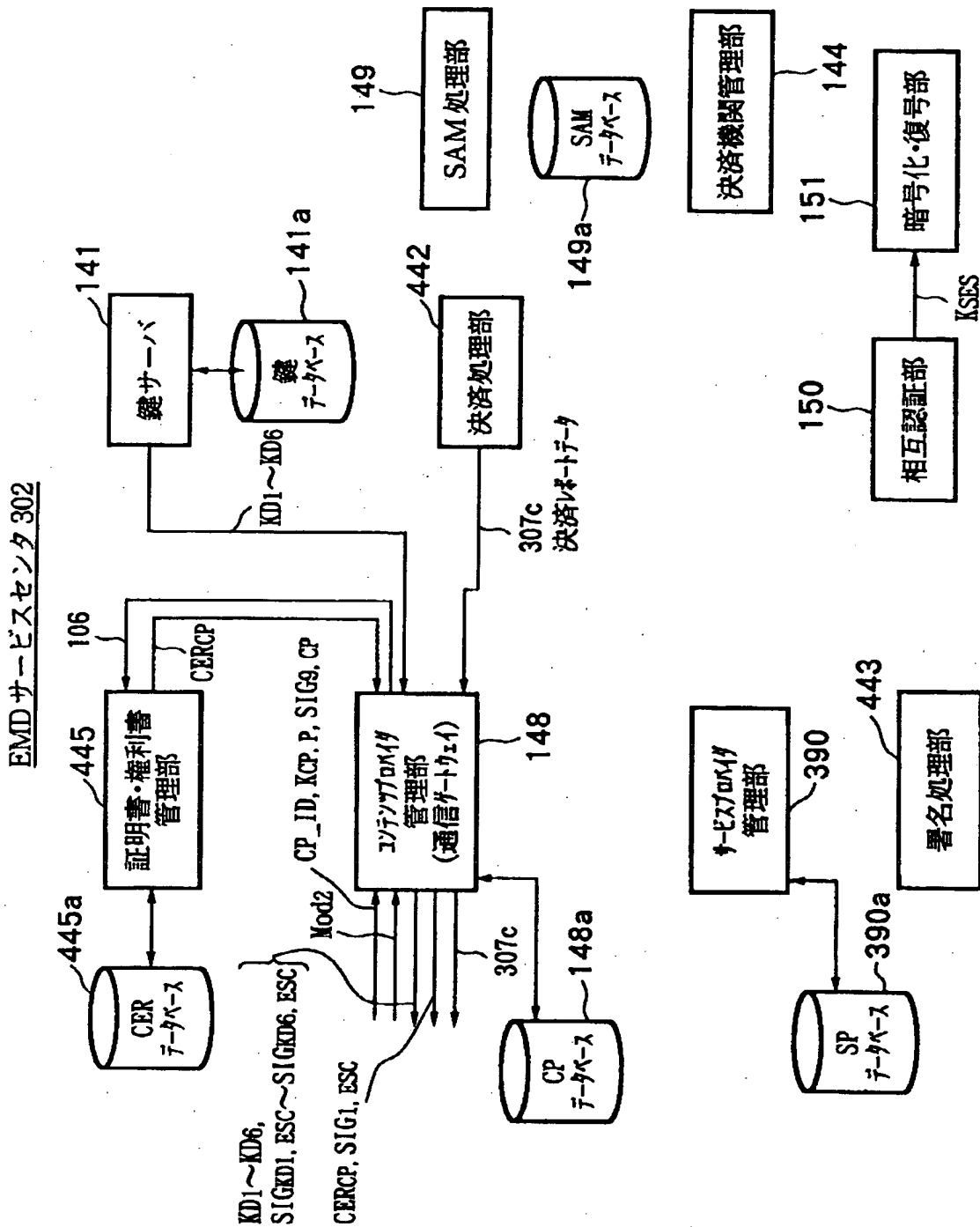
【図 3 7】



【図 38】

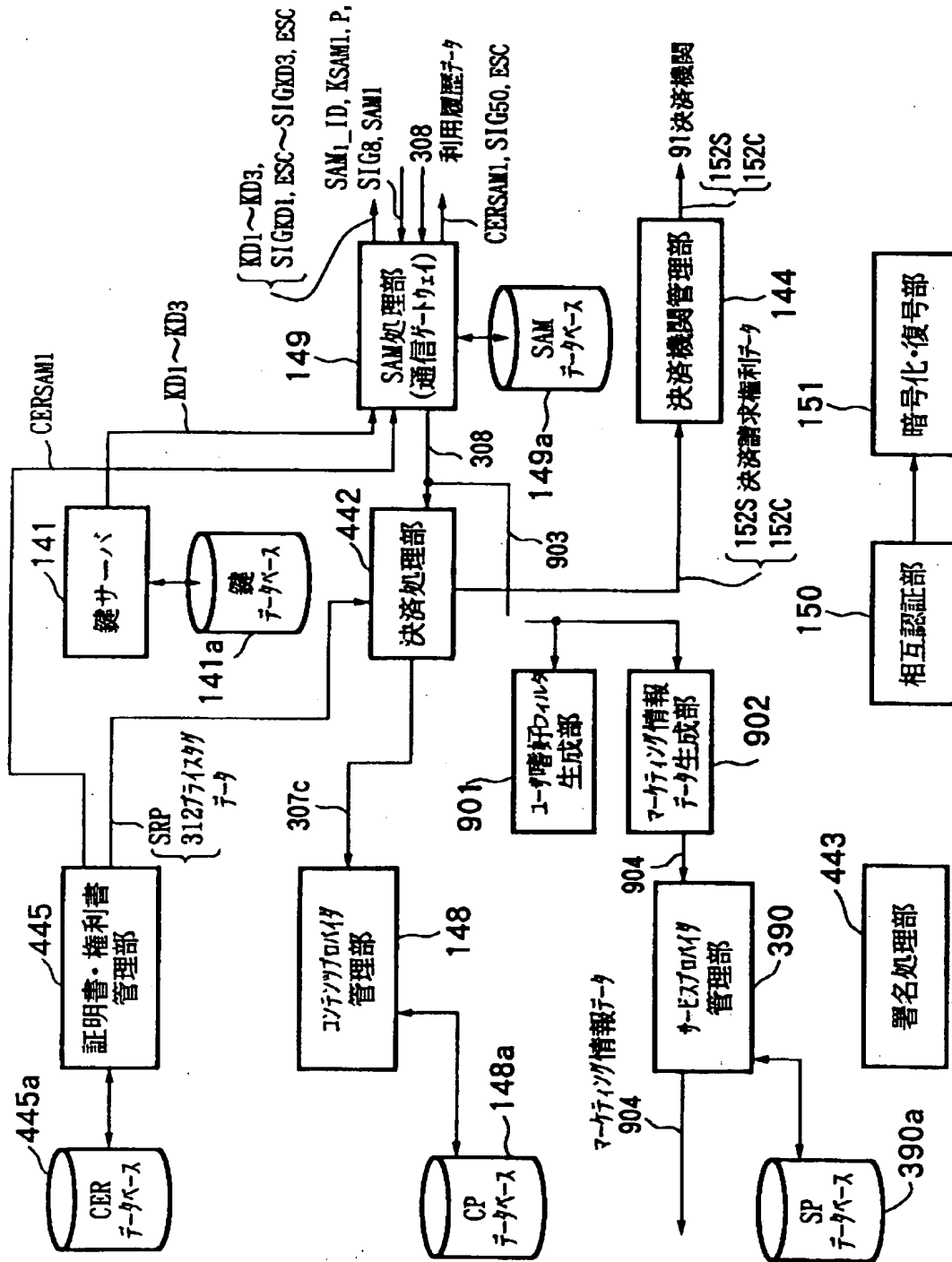


【図 3 9】



【図 40】

EMD サービスセンタ 302



【図 4 1】

利用履歴データ 308 の内容

識別子 Content_ID

識別子 CP_ID

識別子 SP_ID

コンテンツデータ C の信号諸元データ

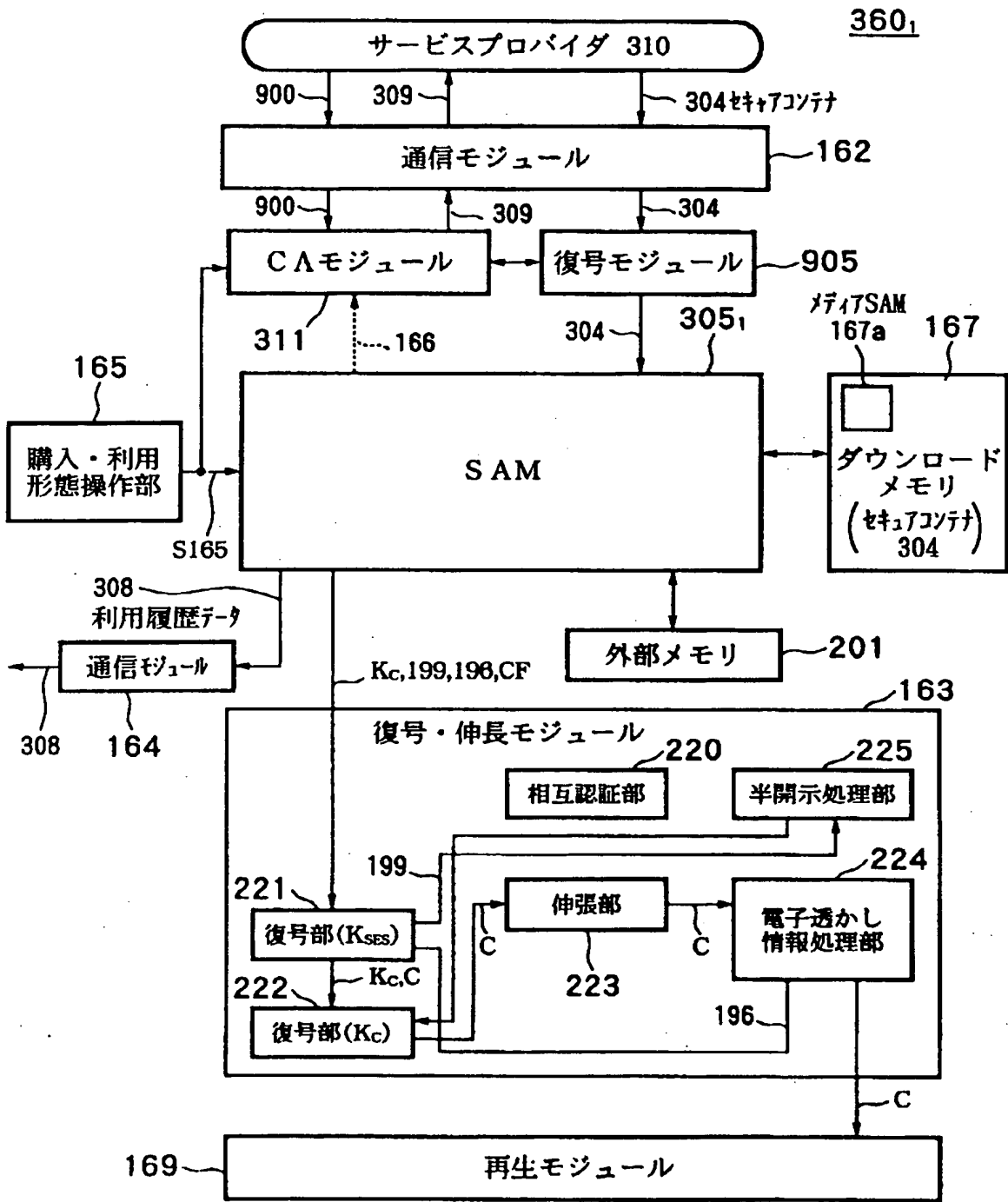
コンテンツデータ C の圧縮方法

記録媒体の識別子 Media_ID

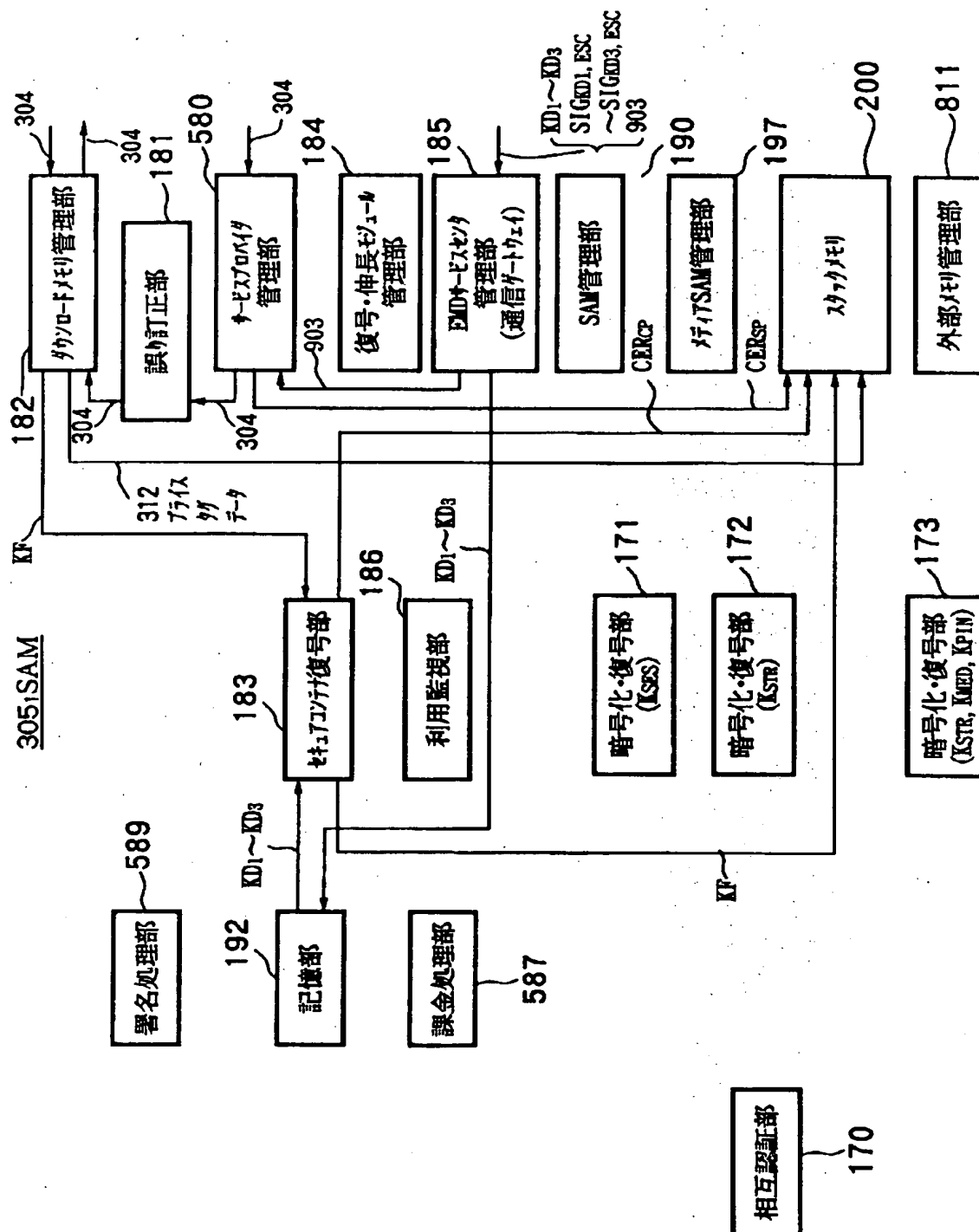
識別子 SAM_ID、

ユーザの USER_ID

【図 4 2】



【图 4-4】

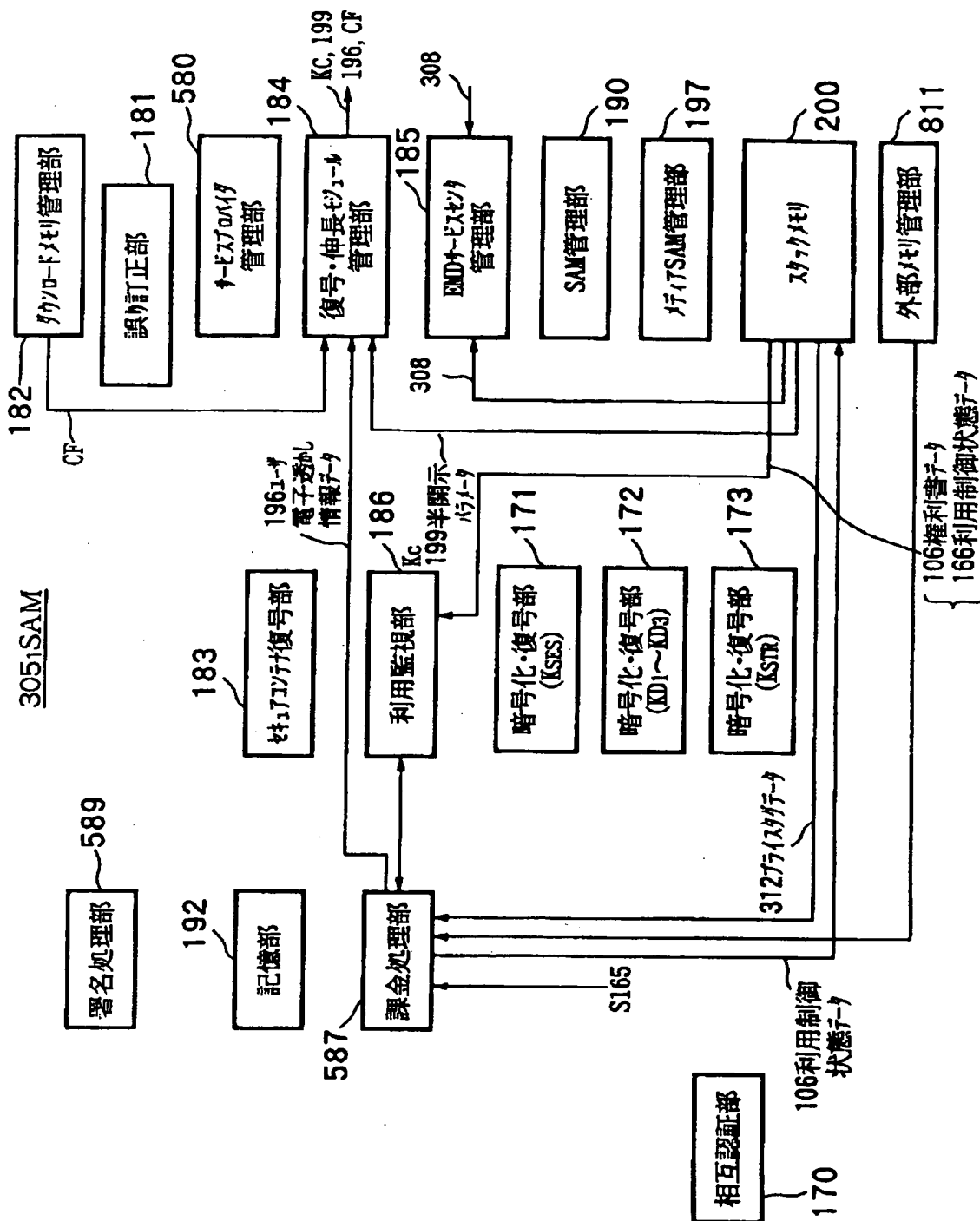


【図 45】

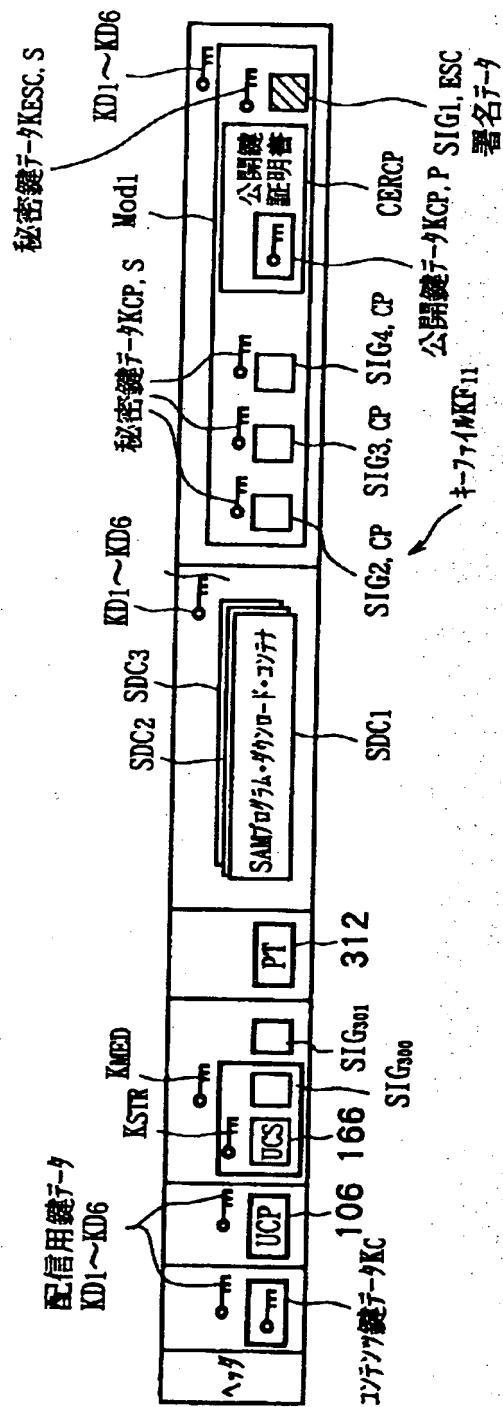
スタックメモリ 200 の記憶データ

コンテンツ鍵データ K_c
権利書データ (UCP) 106
不揮発性メモリ 201 のロック鍵データ K_{Loc}
コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP}
サービスプロバイダ 301 の公開鍵証明書データ CER_{SP}
利用制御情状態データ (UCS) 166
SAM プログラム・ダウンロード・コンテナ $SD_1 \sim SDC_3$
プライスタグデータ 312

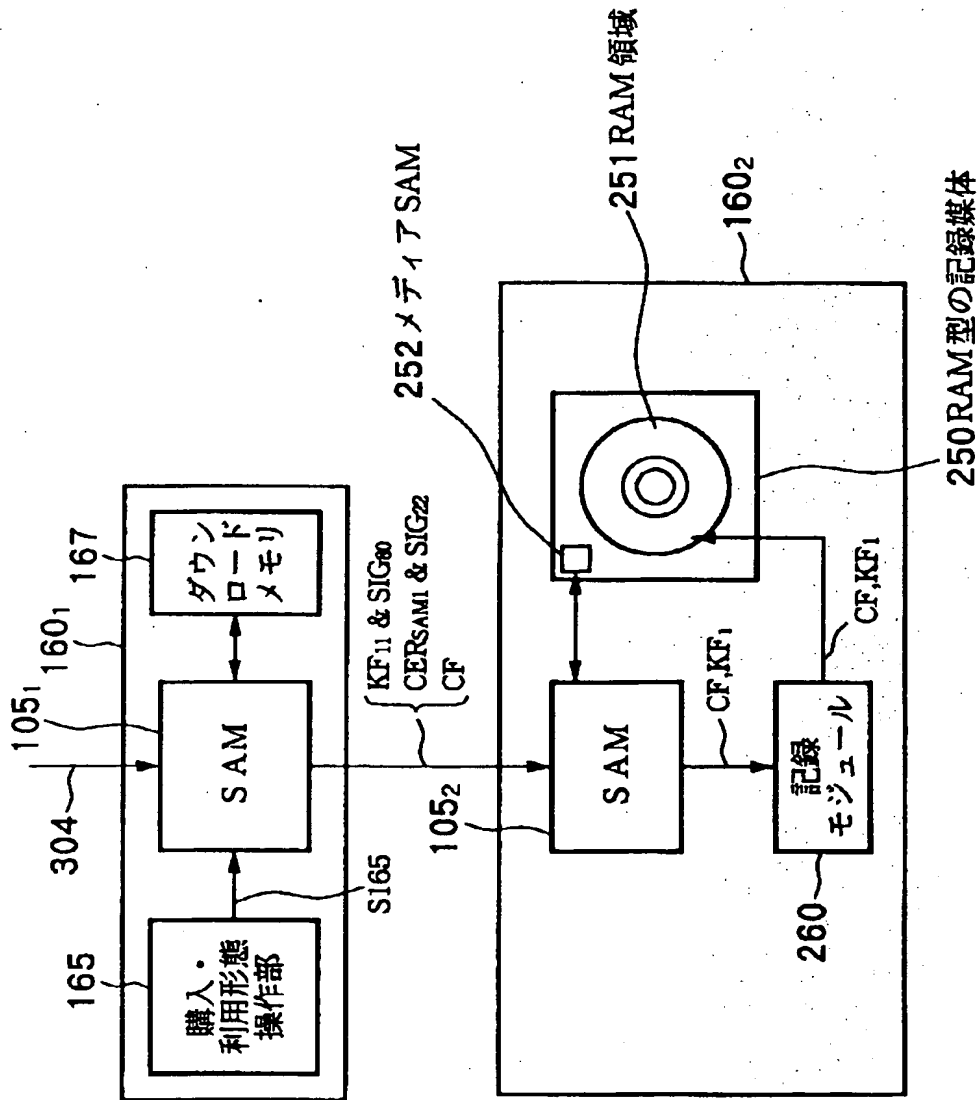
【图 4.6】



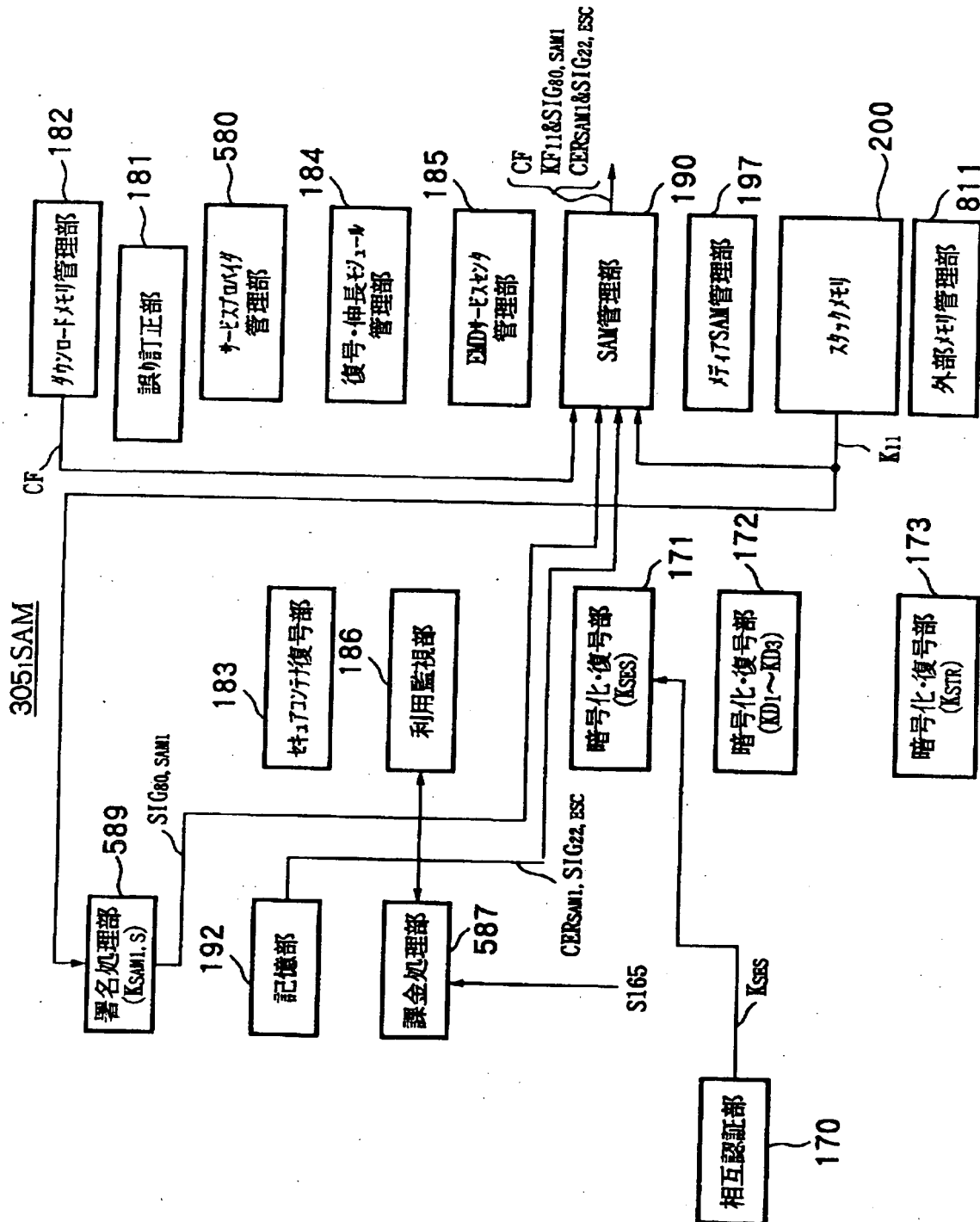
【図 47】



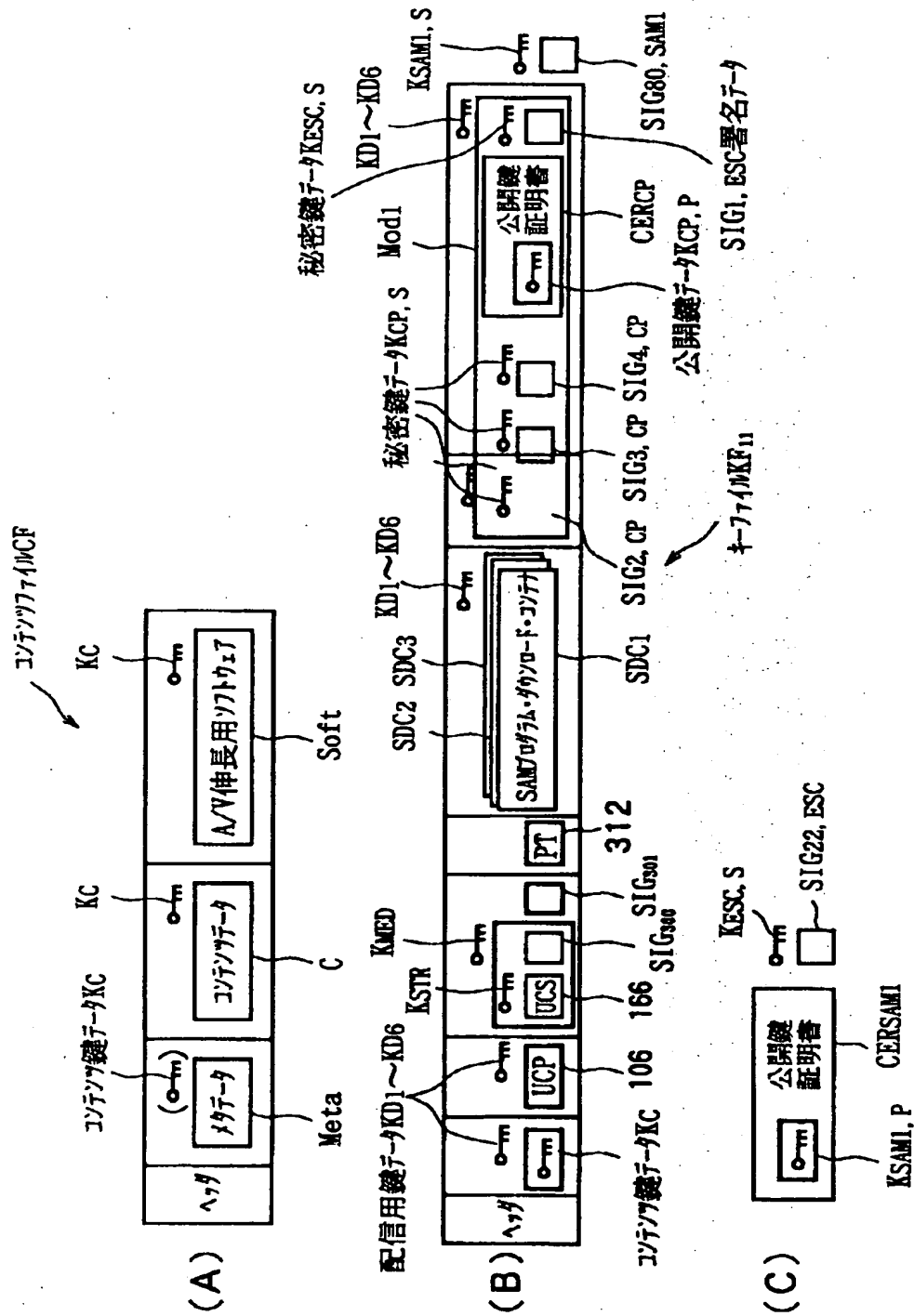
【図 4 8】



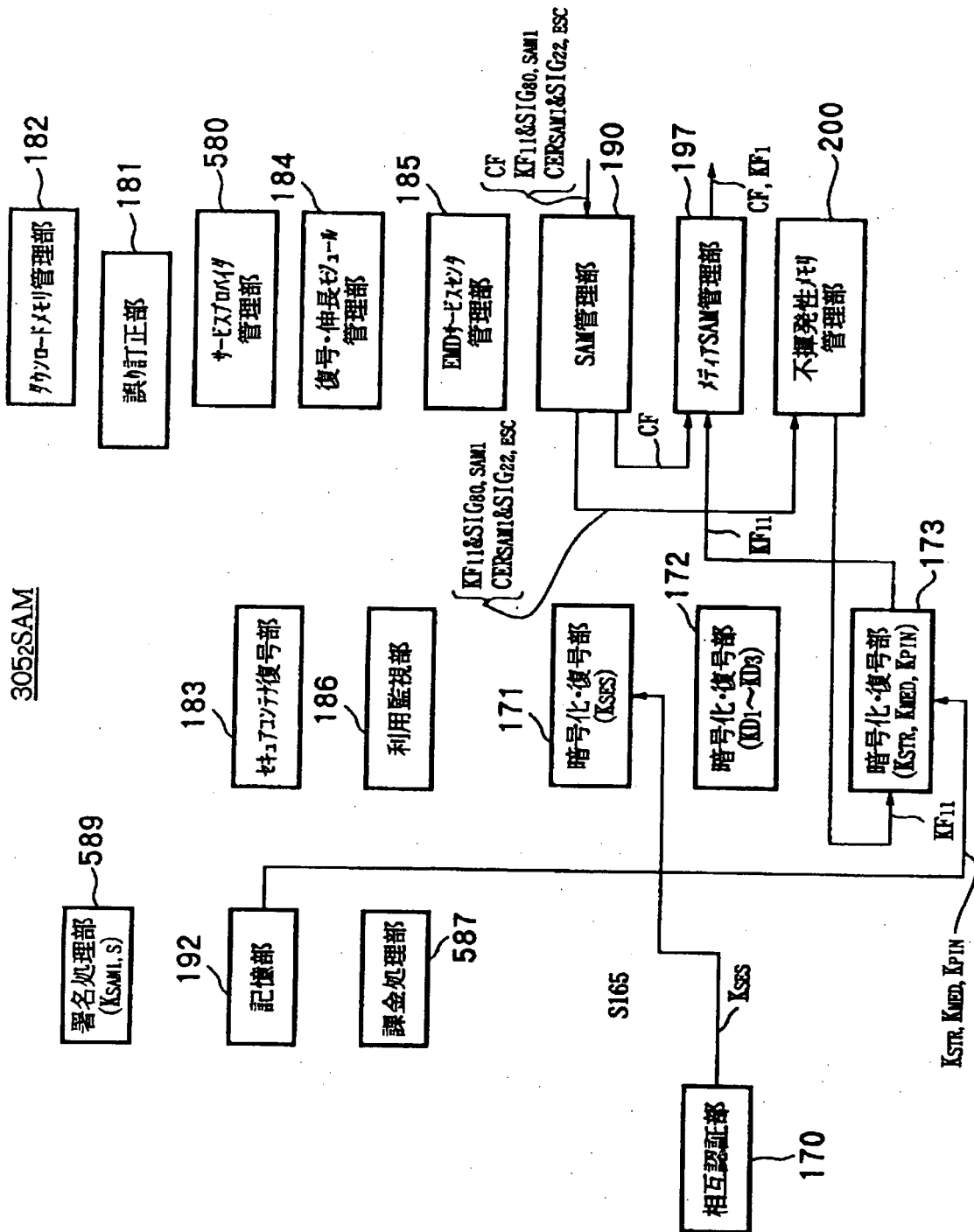
【図 4 9】



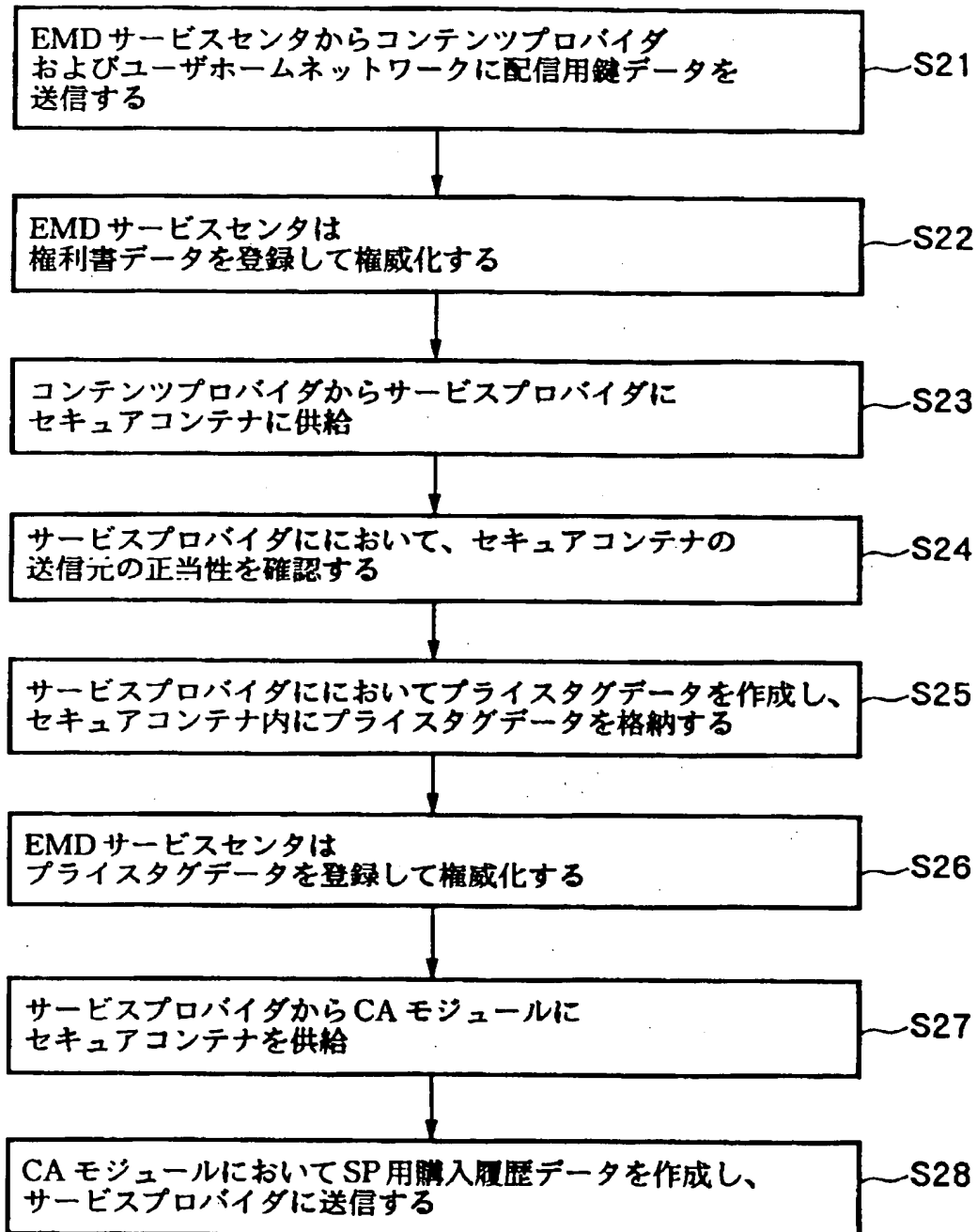
【図 50】



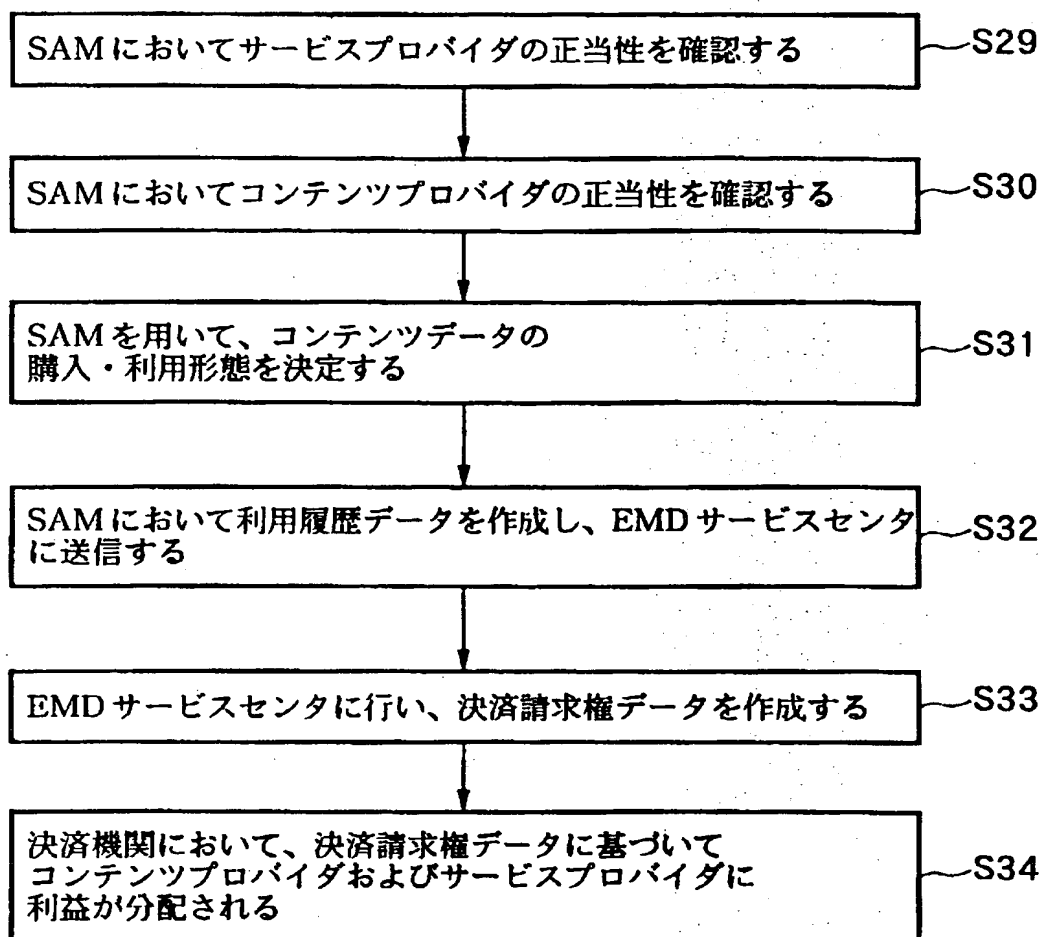
【図 5 1】



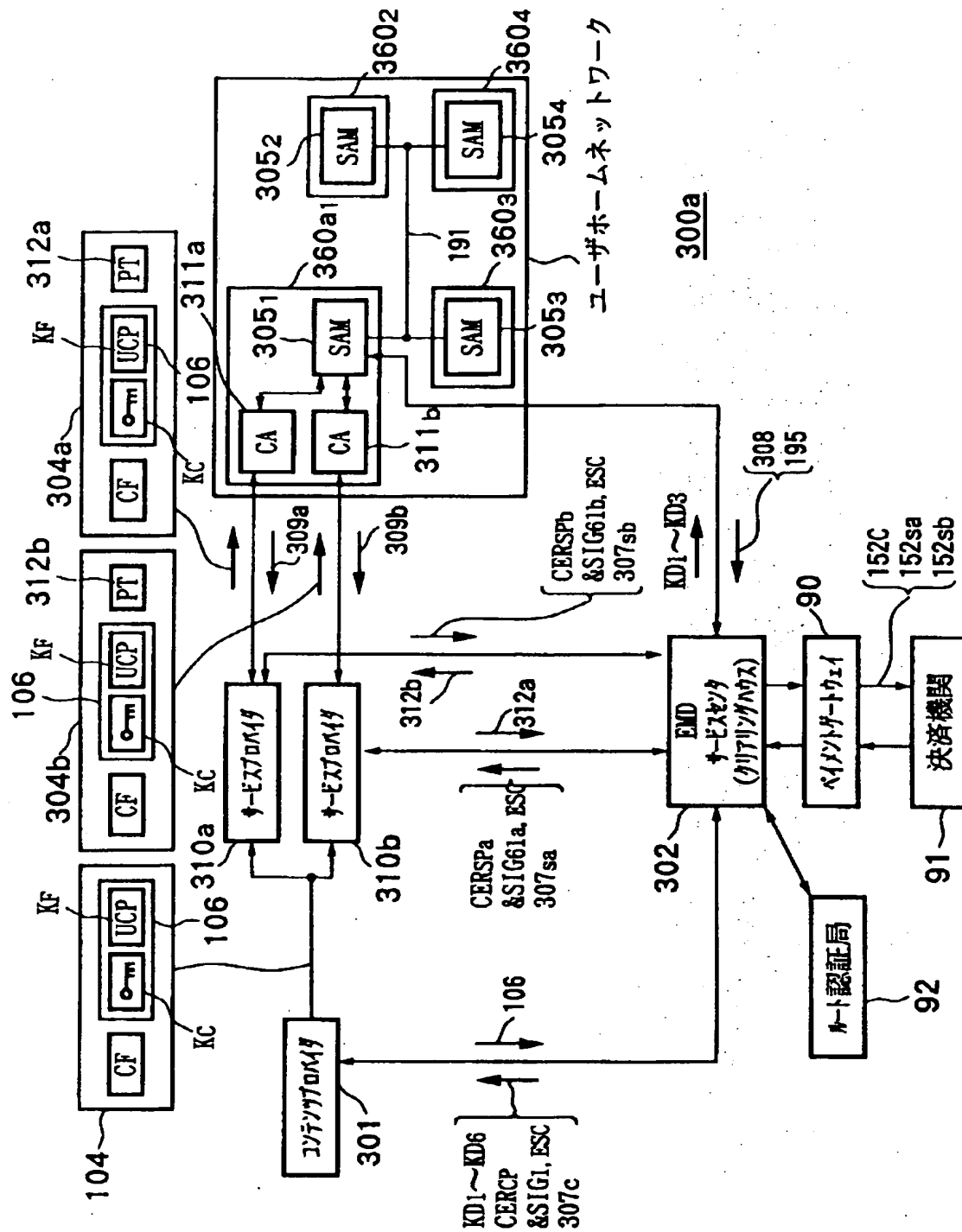
【図 5 2】



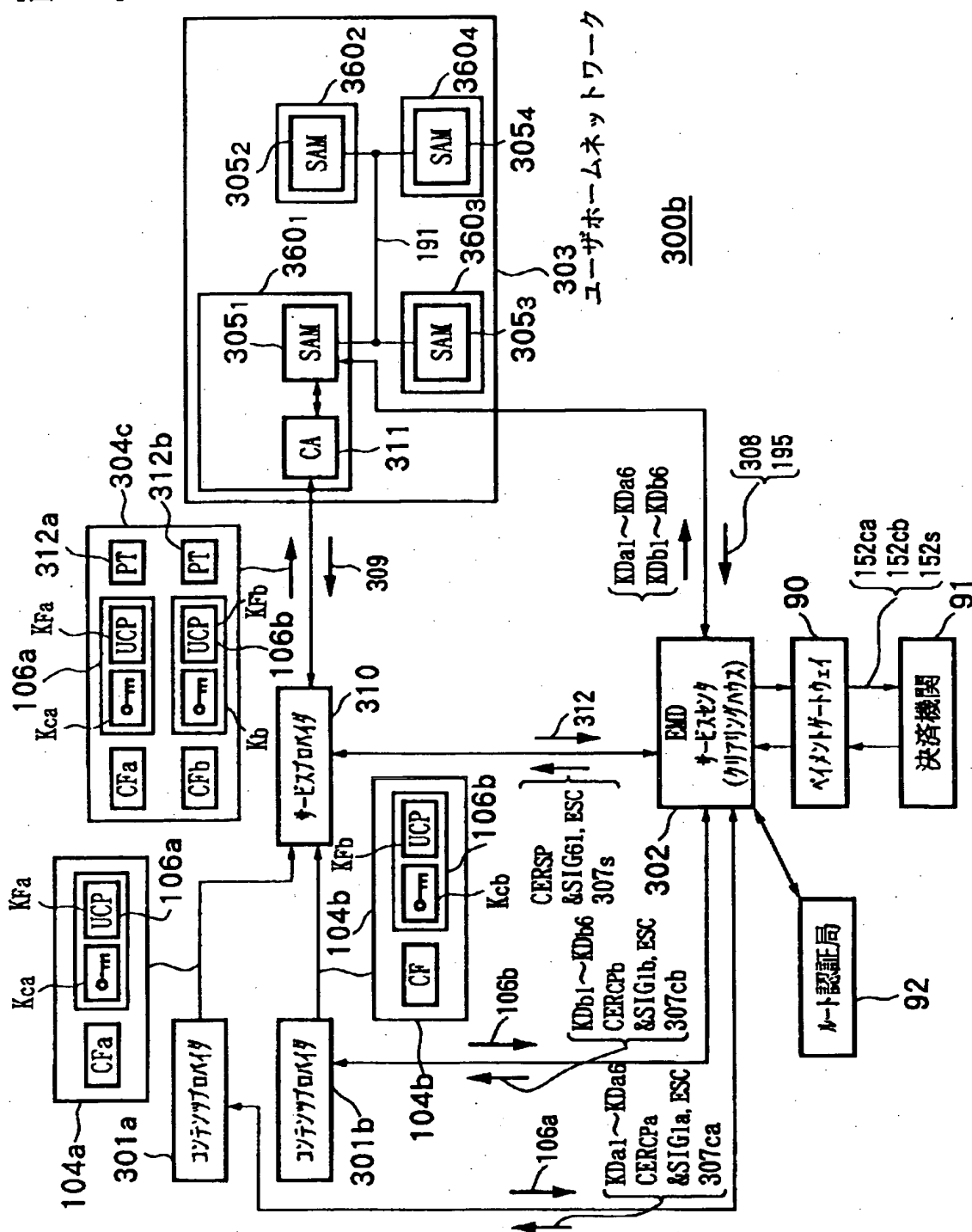
【図 53】



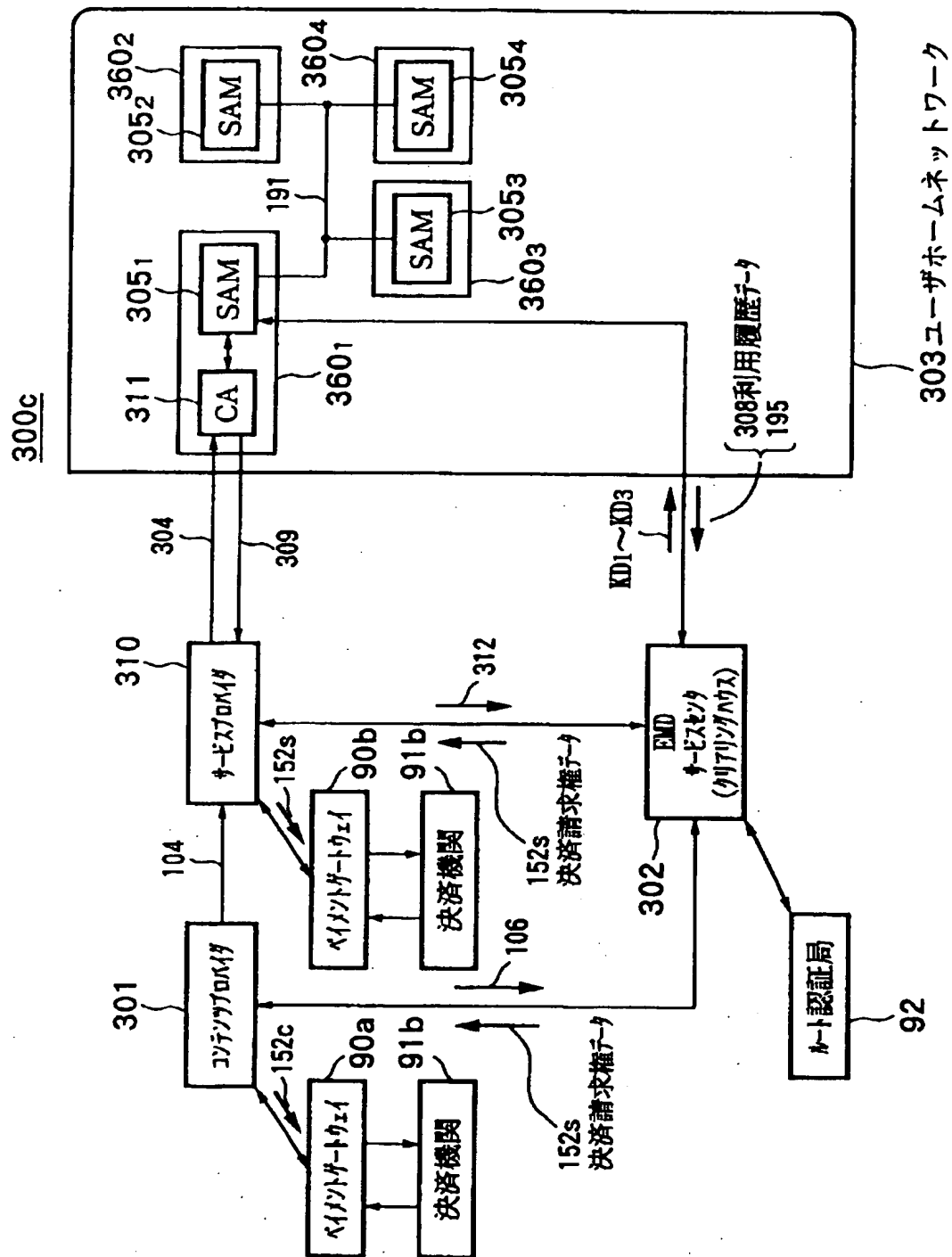
【図 5 4】



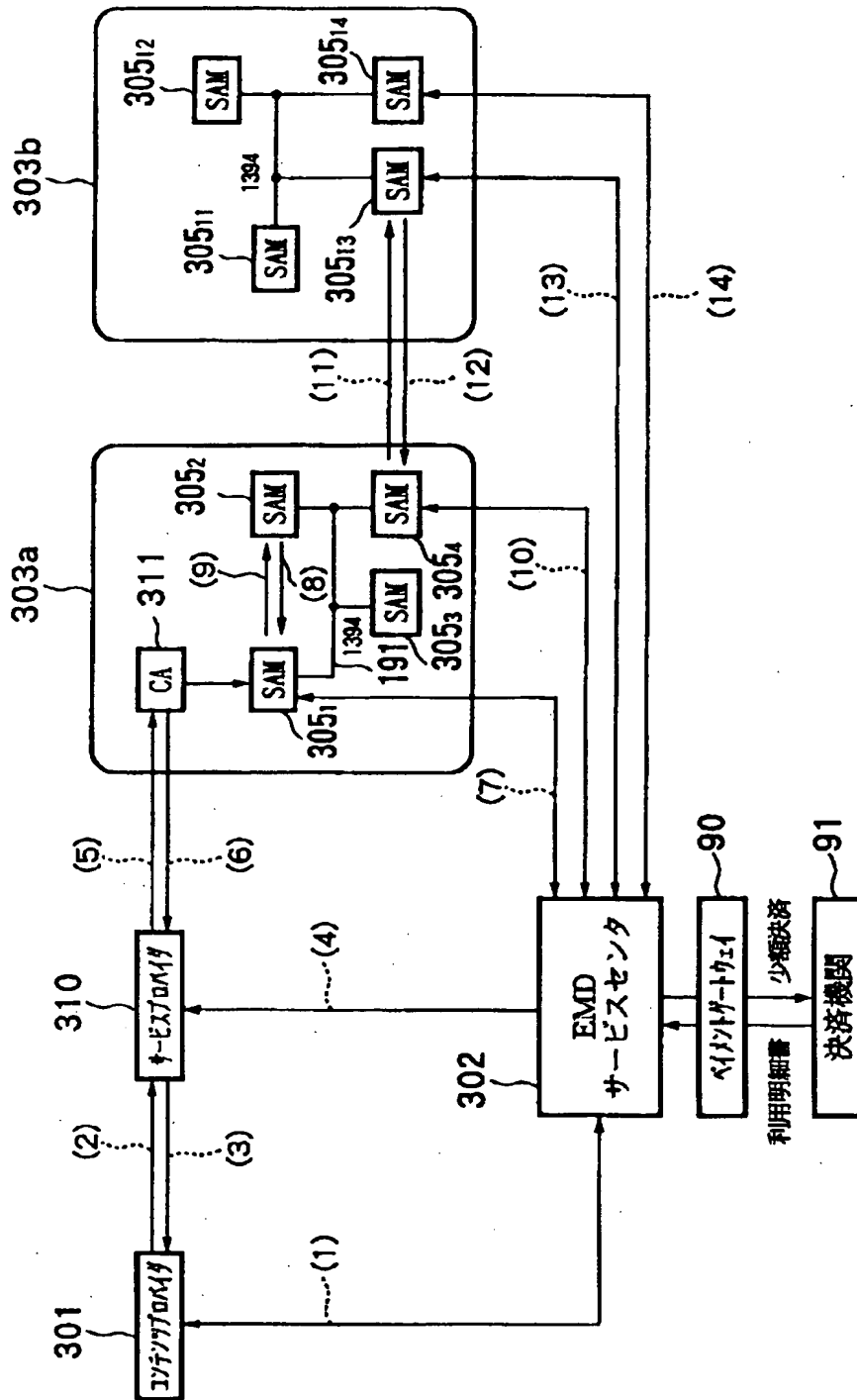
【图 5 5】



【图 5 6】

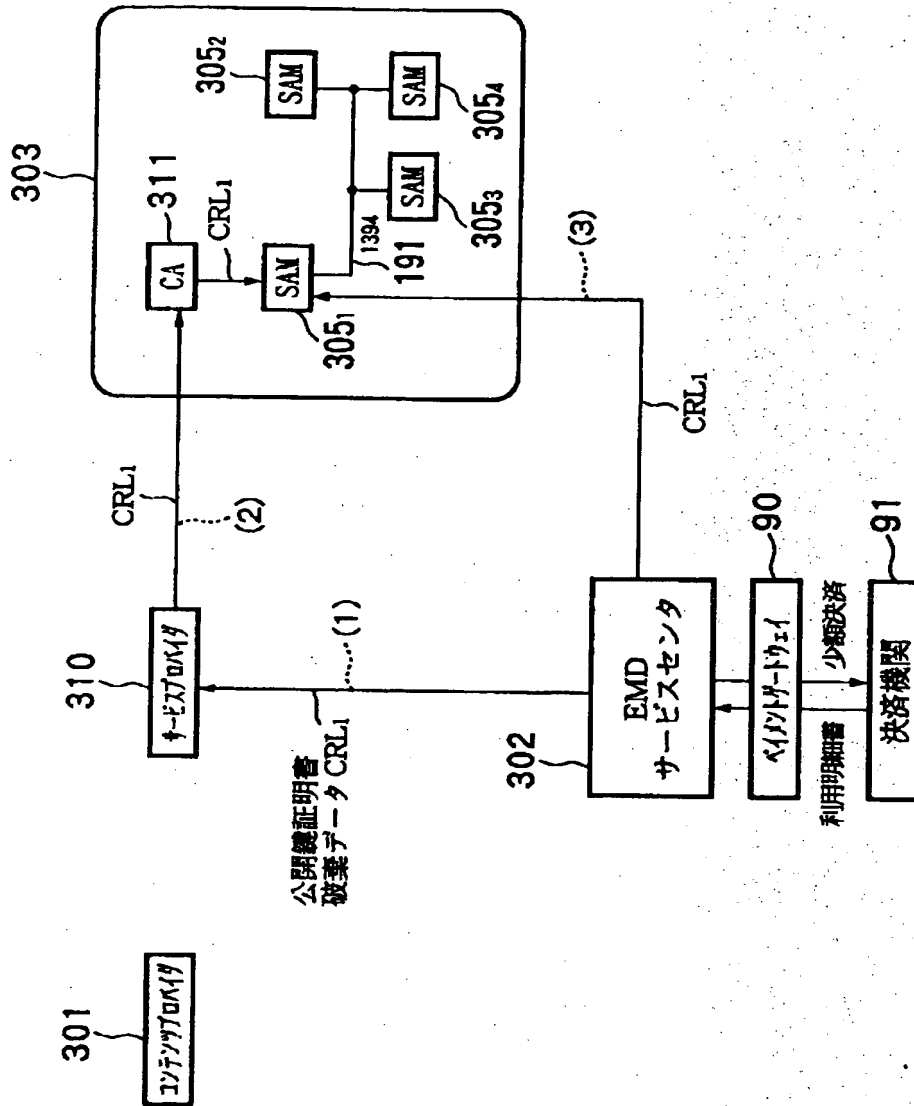


【図 5 8】



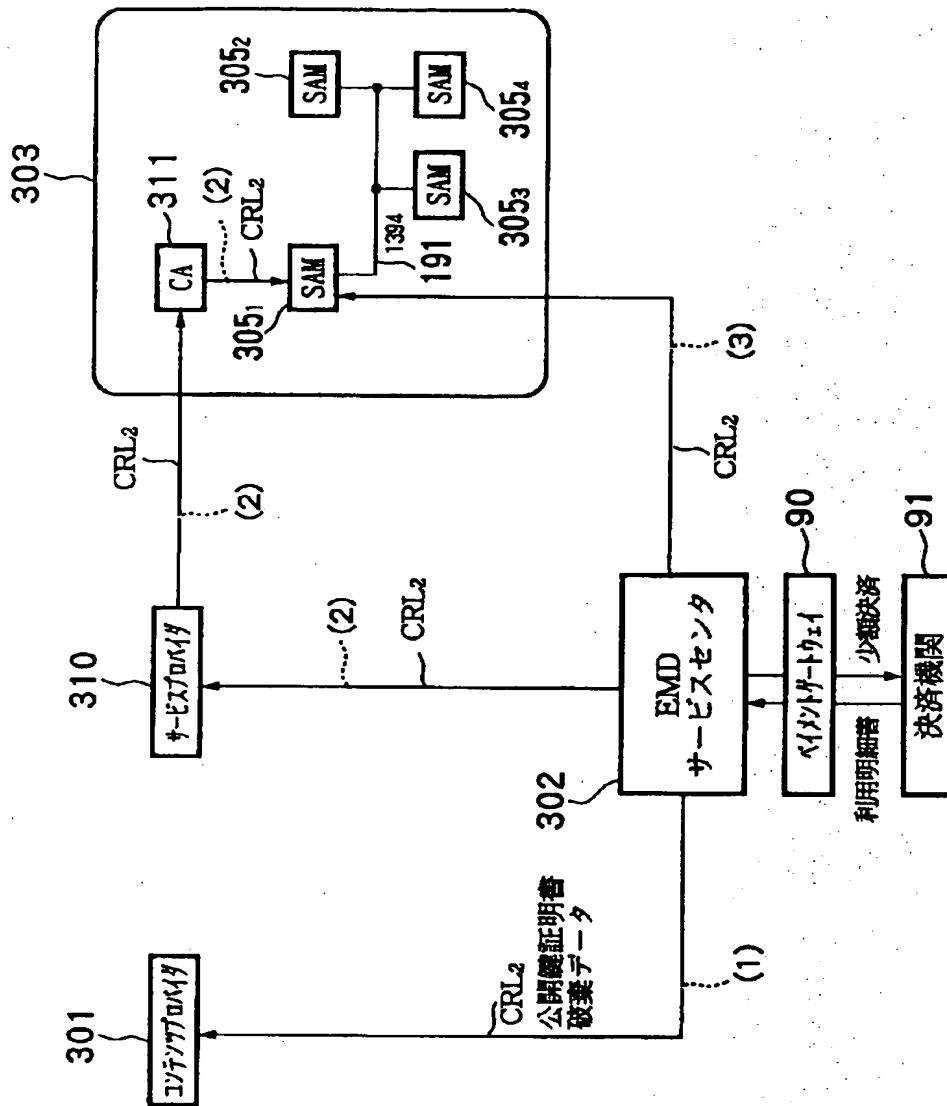
公開鍵証明書の手ルート

【図 5 9】



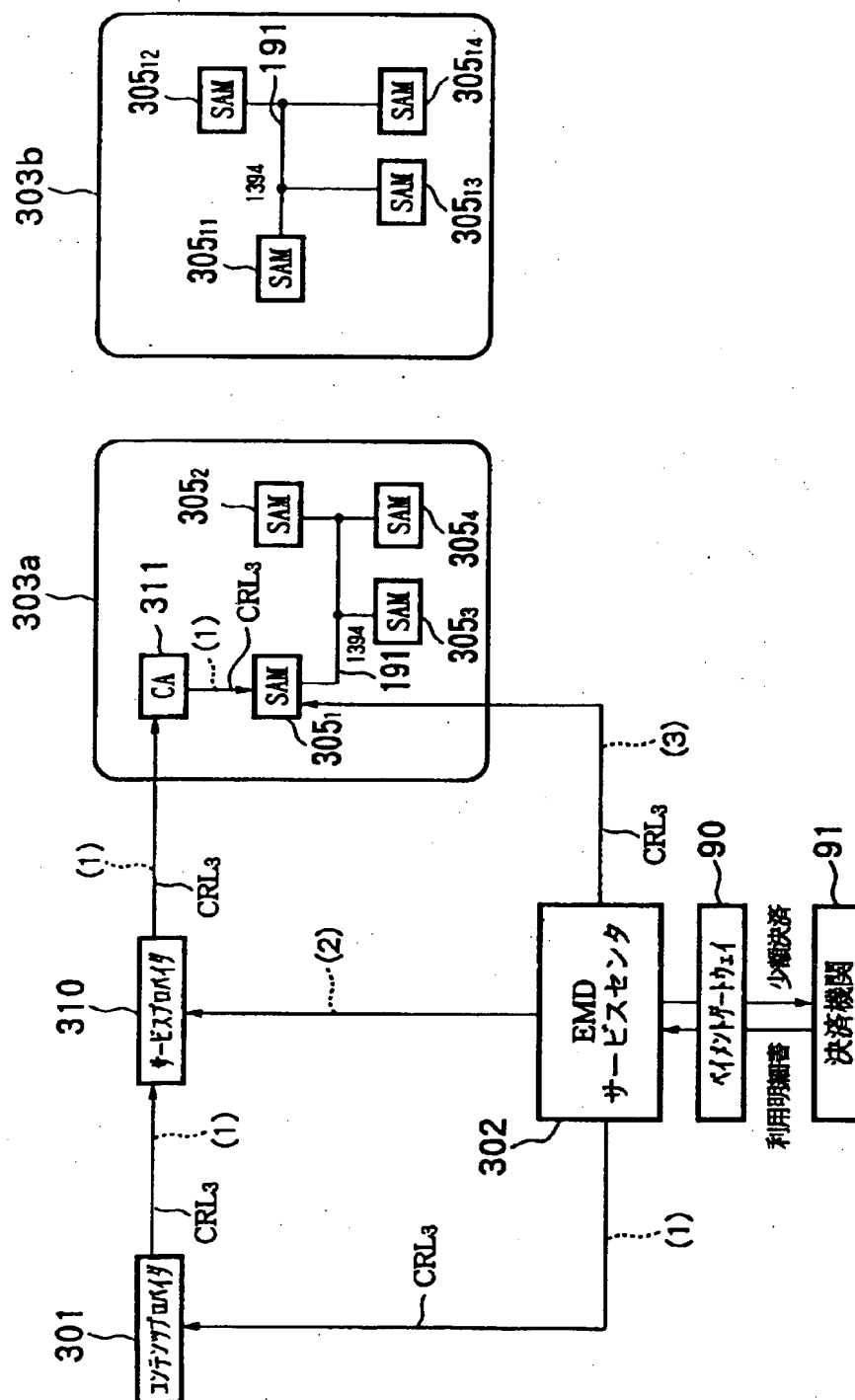
CERCP を無効にする場合

【図 60】



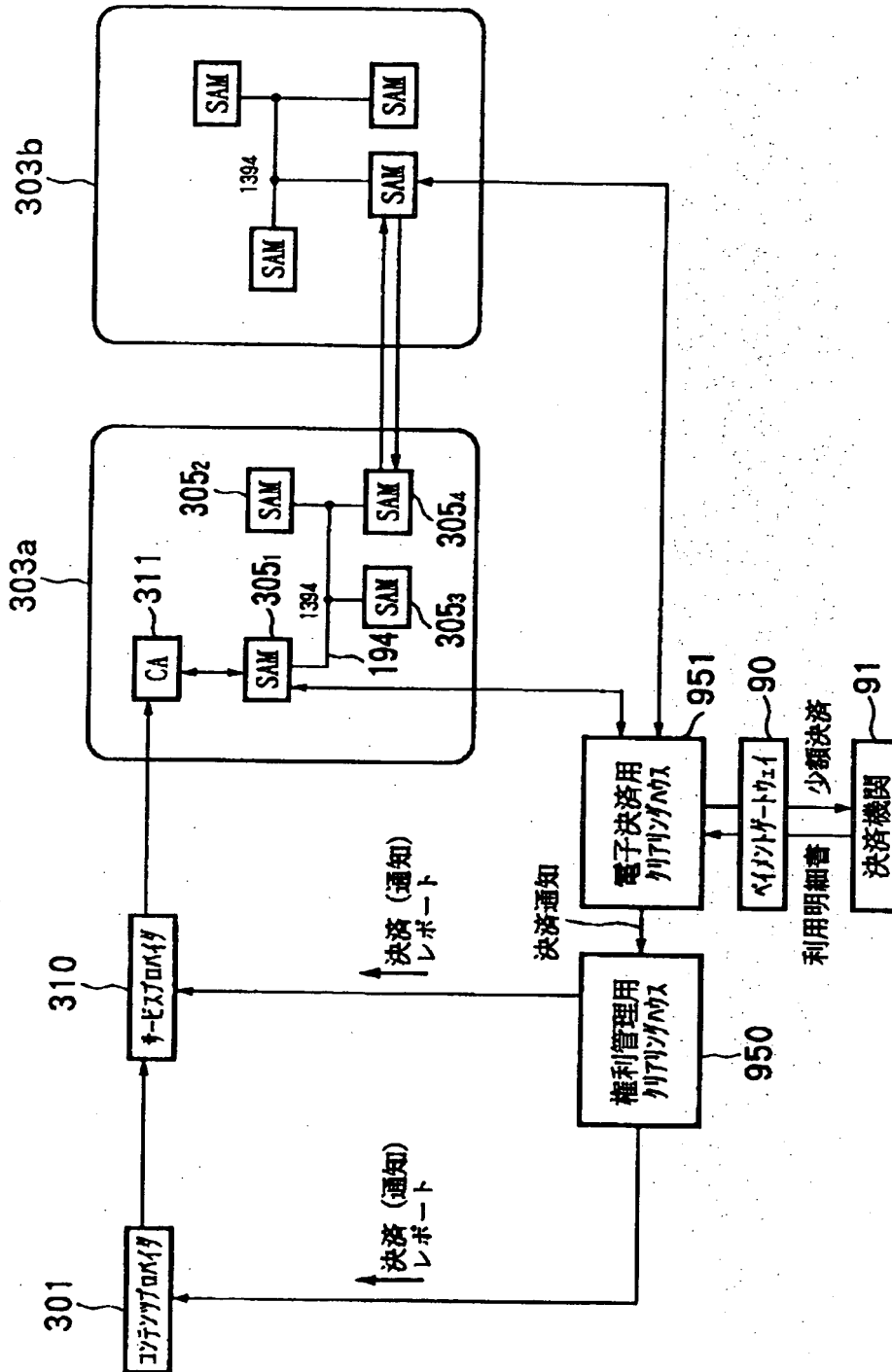
CERSP を無効にする場合

【図 6 1】

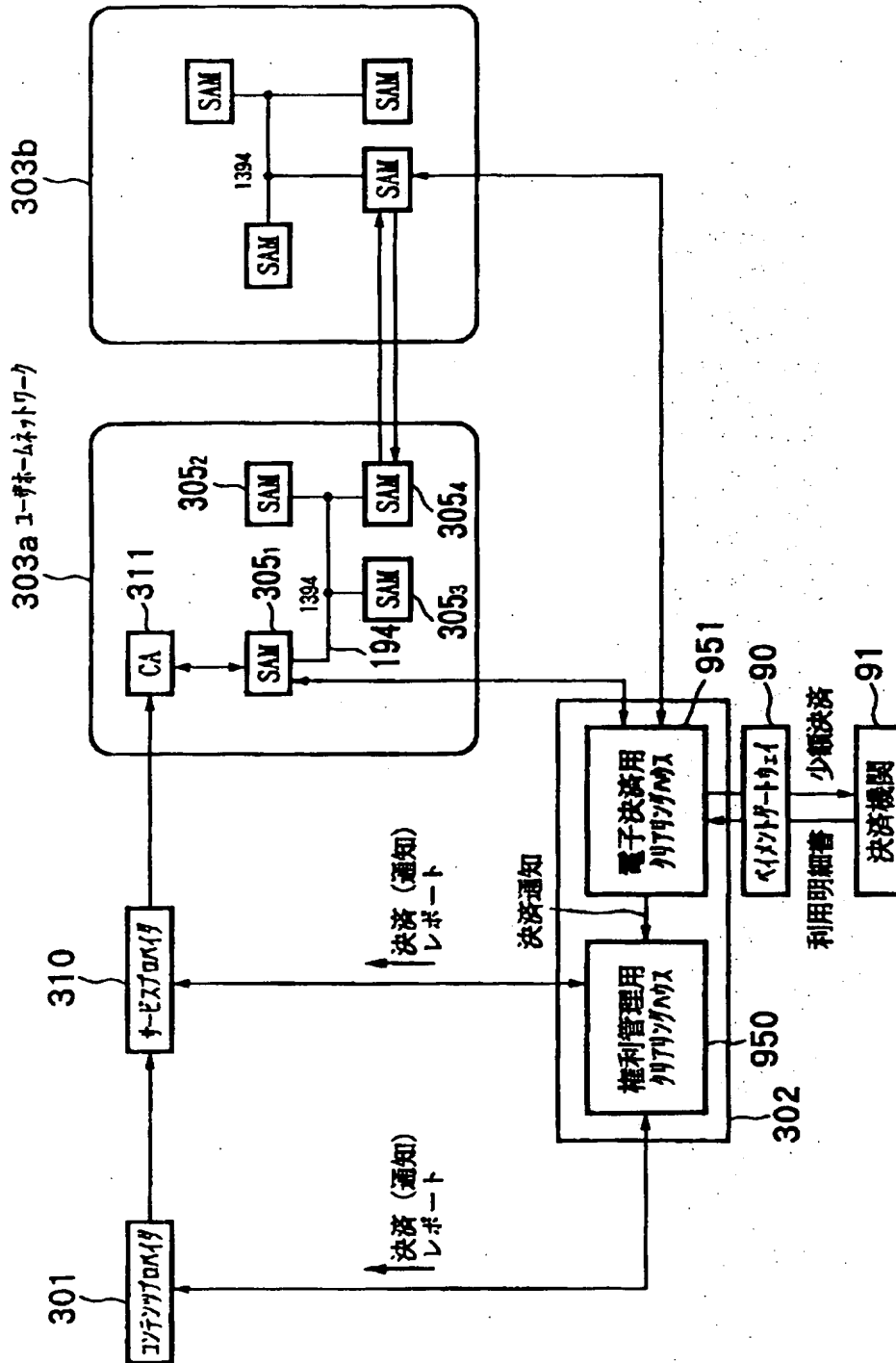


CERSAM2を無効にする場合

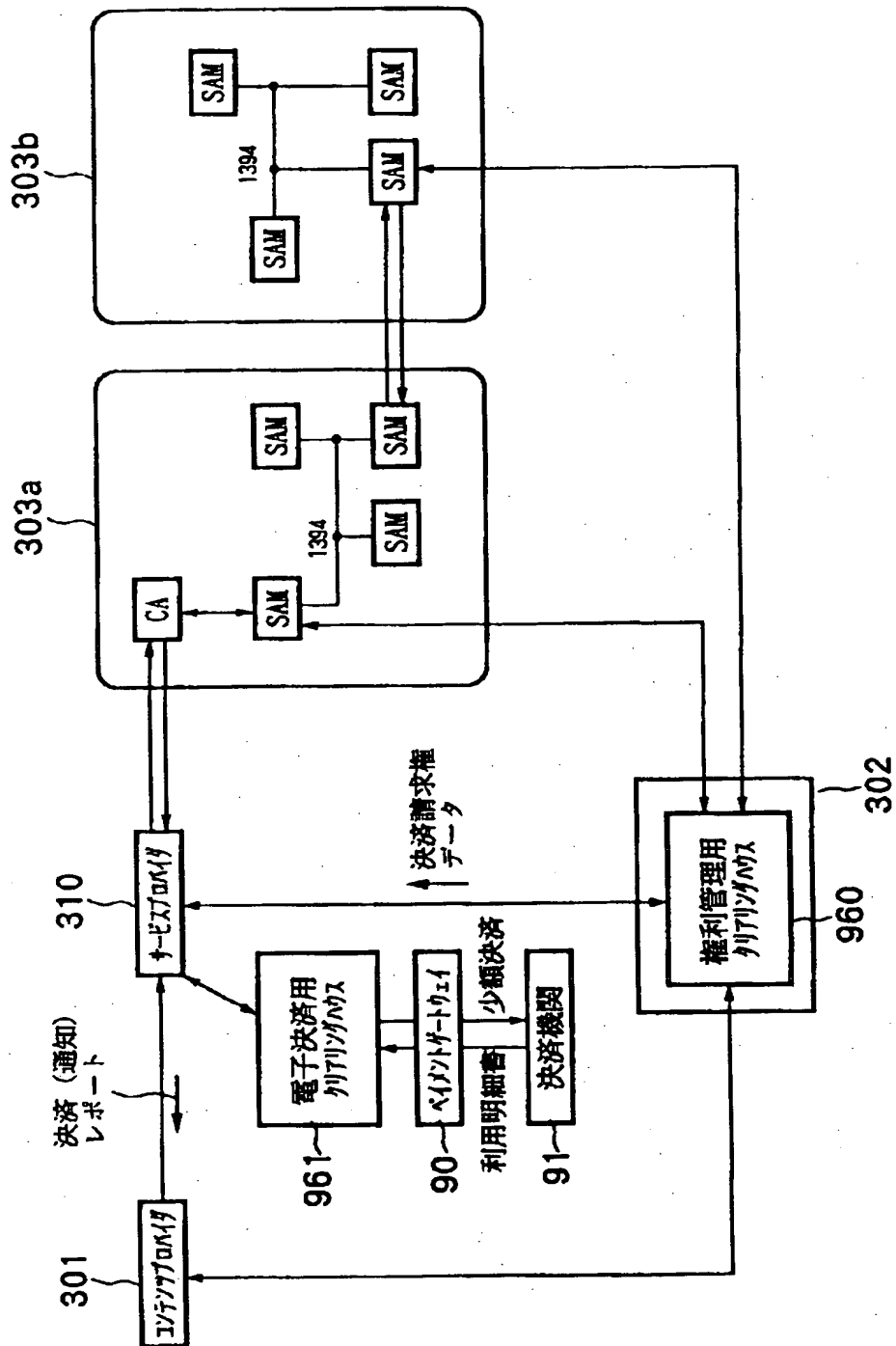
【図 6 3】



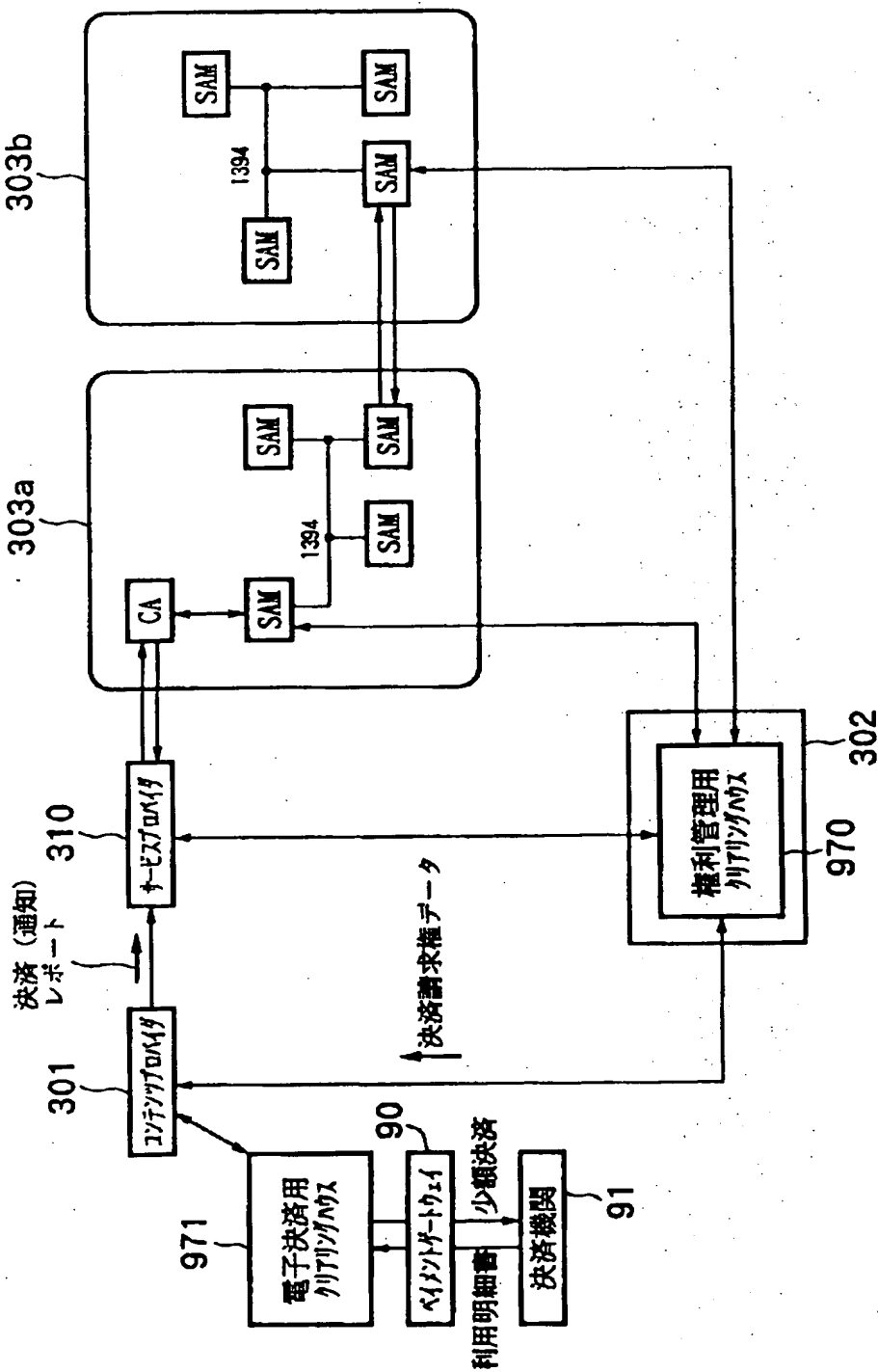
【図 6 4】



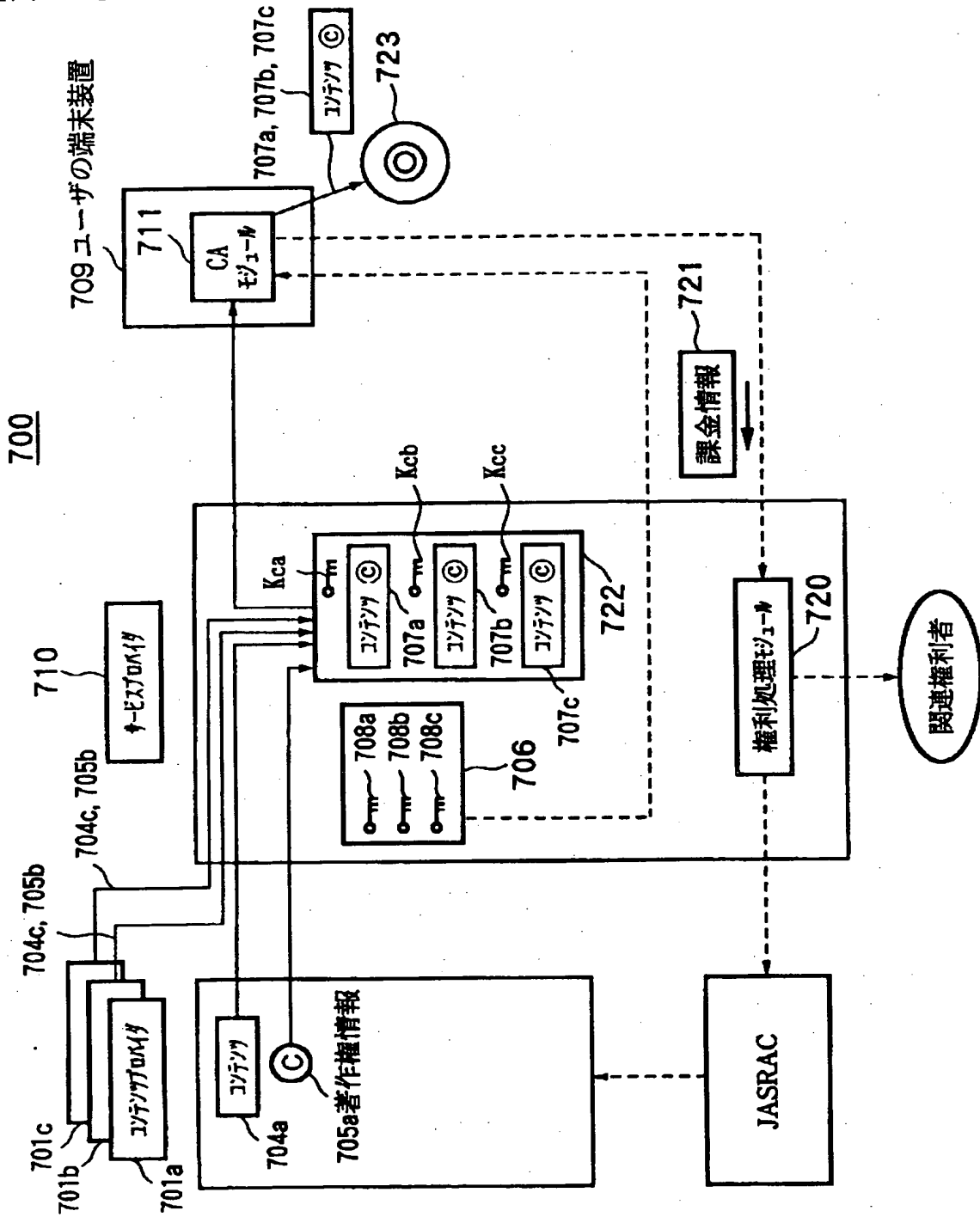
【図 65】



【图 6 6】



【図 67】



【書類名】

要約書

【要約】

【課題】 データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。

【解決手段】 コンテンツプロバイダ101は、コンテンツファイルCFと、コンテンツファイルCFの取り扱いを示す権利書データを格納したキーファイルKFとをユーザホームネットワーク103のSAM105₁～105₄に配給し、権利書データの正当性を証明することをEMDサービスセンタ102に要求する。SAM105₁～105₄は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。EMDサービスセンタ102は、コンテンツプロバイダ101およびSAM105₁～105₄を管理し、コンテンツプロバイダ101からの要求に応じて権利書データの正当性を証明する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社